GDPRiS Platform v2 Guidance for Users

Document Version: 1.0
Revision Date: 09/03/2022

DP Staff

Incident Log

Important Notice:

This document and the associated software are the sole property of GDPRiS. Reproduction or duplication by any means of any portion of this document without the prior written consent of GDPRiS is expressly forbidden.

GDPRiS reserves the right to make changes to this document and to the related software at any time without notice. The information in this document has been carefully checked for its accuracy; however, GDPRiS makes no warranty relating to the correctness of this document.

Contents

Incidents

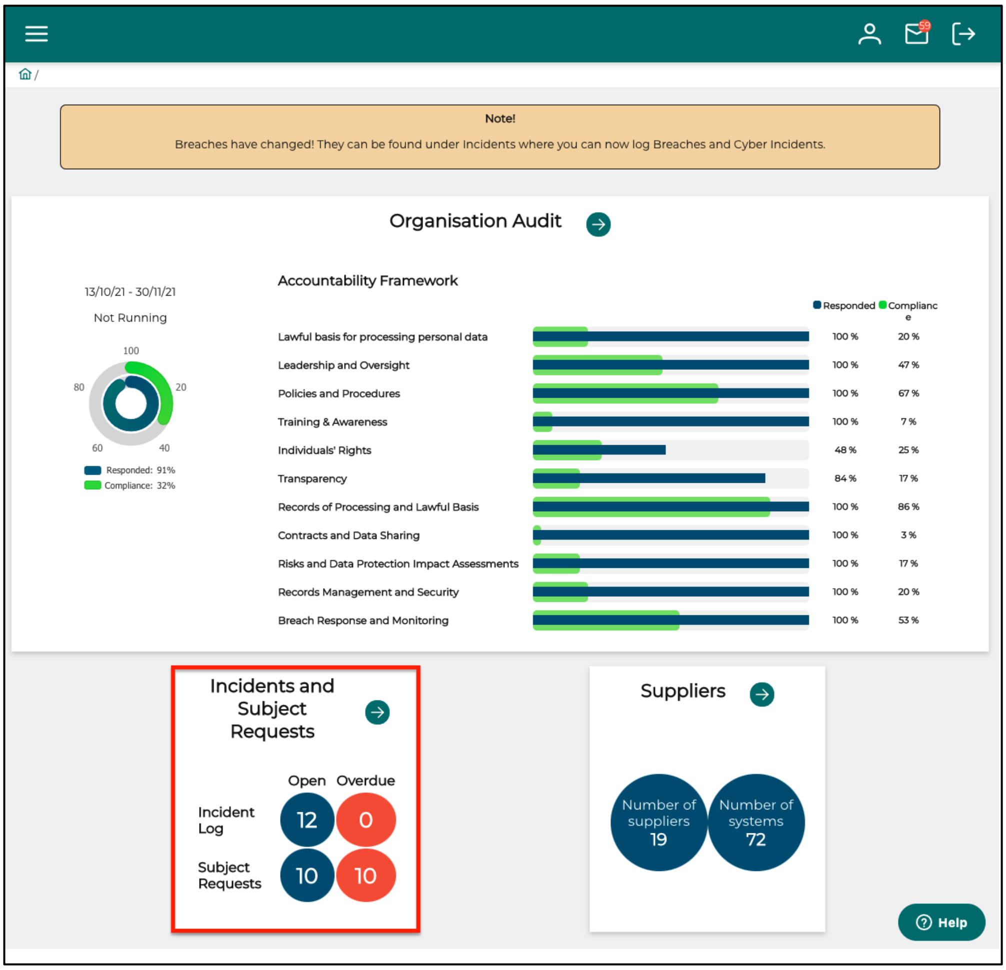
The aim of the Incident Log is to provide you with a central location to manage and process both Data Breaches and Cyber-attacks through its life cycle.

Historically the GDPRiS portal only allowed users to capture information regarding data breaches, now the portal can cater for both data breaches and cyber-attacks. Since both data breaches and cyber-attacks are classed as Incidents, we have introduced a new section called "**Incident Log**".

Incident typical meaning – *"an action likely to lead to grave consequences"*

Access the Incident Management Tool

The Incident Management Tool can be accessed via the navigation menu or via the Incident and Information Requests widget on the school dashboard.



Note!

Breaches have changed! They can be found under Incidents where you can now log Breaches and Cyber Incidents.

Organisation Audit

13/10/21 - 30/11/21

Not Running

Accountability Framework

	Responded	Compliance
Lawful basis for processing personal data	100 %	20 %
Leadership and Oversight	100 %	47 %
Policies and Procedures	100 %	67 %
Training & Awareness	100 %	7 %
Individuals' Rights	48 %	25 %
Transparency	84 %	17 %
Records of Processing and Lawful Basis	100 %	86 %
Contracts and Data Sharing	100 %	3 %
Risks and Data Protection Impact Assessments	100 %	17 %
Records Management and Security	100 %	20 %
Breach Response and Monitoring	100 %	53 %

Incidents and Subject Requests

	Open	Overdue
Incident Log	12	0
Subject Requests	10	10

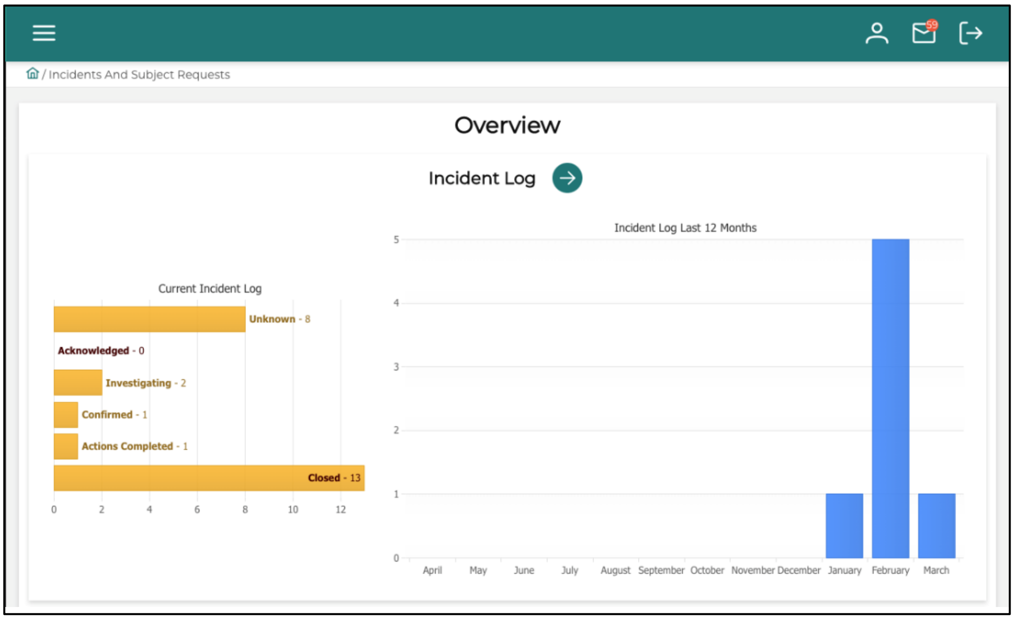
Suppliers

Number of suppliers 19

Number of systems 72

Overview

The Incidents and Subject Requests Overview page provides counts on the Incidents raised across a twelve-month period and the status of the Incidents.

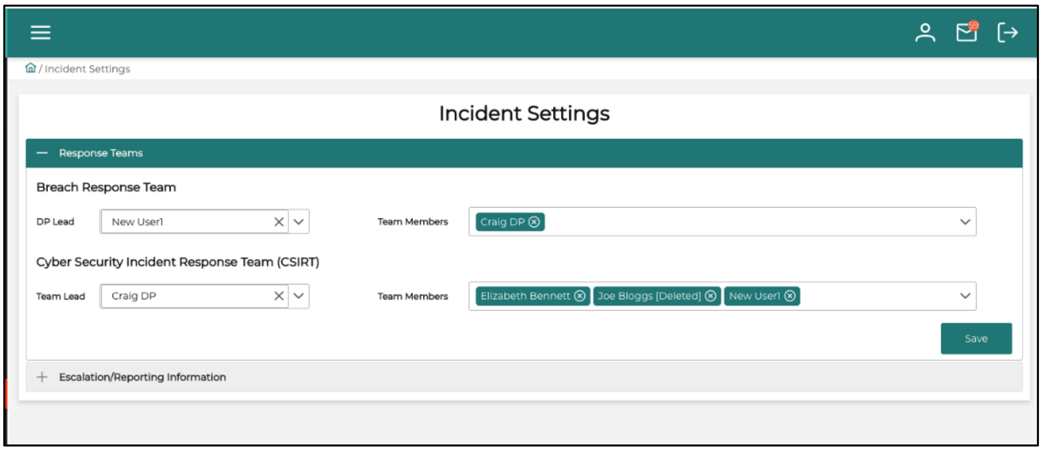


Incident Settings

When incidents are raised, certain members of your organisation should be made aware so that the correct people can start to investigate and manage them. This can be done via the “**Incident Settings**” which can be accessed via the navigation menu down the left-hand side under “**Incidents and Subject Requests**”.

Response Teams

In the Incident Settings you can select your DP Lead for Data Breaches and your Team Lead for Cyber Incidents as well as their team members.



Breach Response Team

DP Lead: New User1 — Team Members: Craig DP

Cyber Security Incident Response Team (CSIRT)

Team Lead: Craig DP — Team Members: Elizabeth Bennett, Joe Bloggs [Deleted], New User1

Important Note: When an incident is raised, depending on the type of incident and if you have added Leads and Team Members for data breaches and cyber incidents, those users will be notified via an email that an incident has been raised in the GDPRiS portal and will be prompted to investigate it.

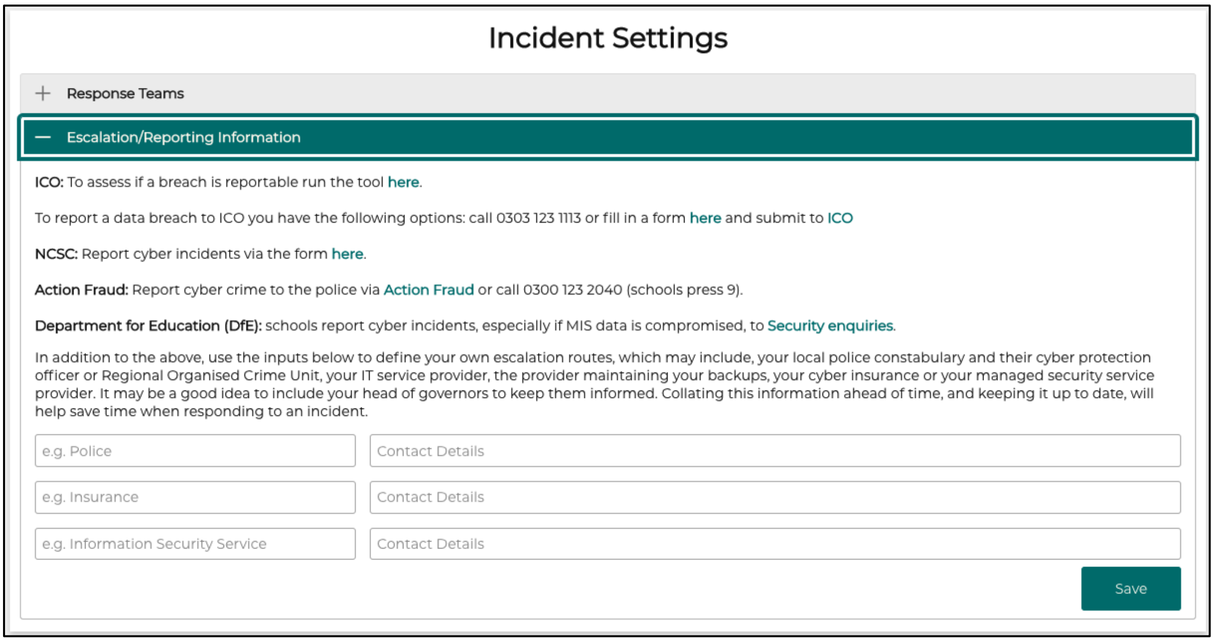
If the DP Lead is the head of both groups they get notified of both breaches and cyber incidents.

If this section is not filled in, all School DP Staff users will receive an email.

If an incident is logged without the breach or cyber box ticked the notification will go to all DP leads in both the Breach and the Cyber Response Teams and then once a DP lead has ticked the relevant box only the relevant response teams will be notified.

Escalation/Reporting Information

In the **Incident Settings** you can add your contacts for points of escalation such as Police, Insurance and Information and Security Service providers.



Incident Settings

ICO: To assess if a breach is reportable run the tool here.

To report a data breach to ICO you have the following options: call 0303 123 1113 or fill in a form here and submit to ICO

NCSC: Report cyber incidents via the form here.

Action Fraud: Report cyber crime to the police via Action Fraud or call 0300 123 2040 (schools press 9).

Department for Education (DfE): schools report cyber incidents, especially if MIS data is compromised, to Security enquiries.

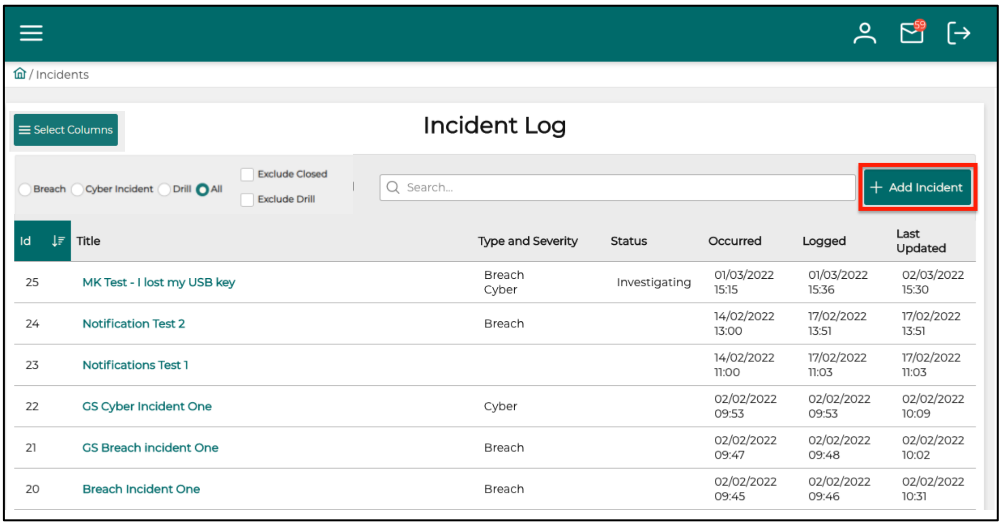
In addition to the above, use the inputs below to define your own escalation routes, which may include, your local police constabulary and their cyber protection officer or Regional Organised Crime Unit, your IT service provider, the provider maintaining your backups, your cyber insurance or your managed security service provider. It may be a good idea to include your head of governors to keep them informed. Collating this information ahead of time, and keeping it up to date, will help save time when responding to an incident.

e.g. Police	Contact Details
e.g. Insurance	Contact Details
e.g. Information Security Service	Contact Details

Links are provided for the **ICO, NCSC (National Cyber Security Centre)** incidents form and the **Police** for their Action Fraud forms as well as the **DfE (Department for Education)** for security queries.

How to log an Incident

To create a new Incident record, simply navigate to the Incident Log page by clicking on “**Incidents and Subject Requests**” and then “**Incident Log**”. You will then be able to click on “**Add Incident**” in the top right-hand corner of the page.



/ Incidents

Select Columns

Incident Log

○ Breach ○ Cyber Incident ○ Drill ● All

□ Exclude Closed

□ Exclude Drill

Search...

+ Add Incident

Id	Title	Type and Severity	Status	Occurred	Logged	Last Updated
25	MK Test - I lost my USB key	Breach Cyber	Investigating	01/03/2022 15:15	01/03/2022 15:36	02/03/2022 15:30
24	Notification Test 2	Breach		14/02/2022 13:00	17/02/2022 13:51	17/02/2022 13:51
23	Notifications Test 1			14/02/2022 11:00	17/02/2022 11:03	17/02/2022 11:03
22	GS Cyber Incident One	Cyber		02/02/2022 09:53	02/02/2022 09:53	02/02/2022 10:09
21	GS Breach incident One	Breach		02/02/2022 09:47	02/02/2022 09:48	02/02/2022 10:02
20	Breach Incident One	Breach		02/02/2022 09:45	02/02/2022 09:46	02/02/2022 10:31

Fill in the relevant information required:

Discovered – When the Incident came to the attention of a member of staff.

Title – A rough descriptive title which identifies what the incident refers to.

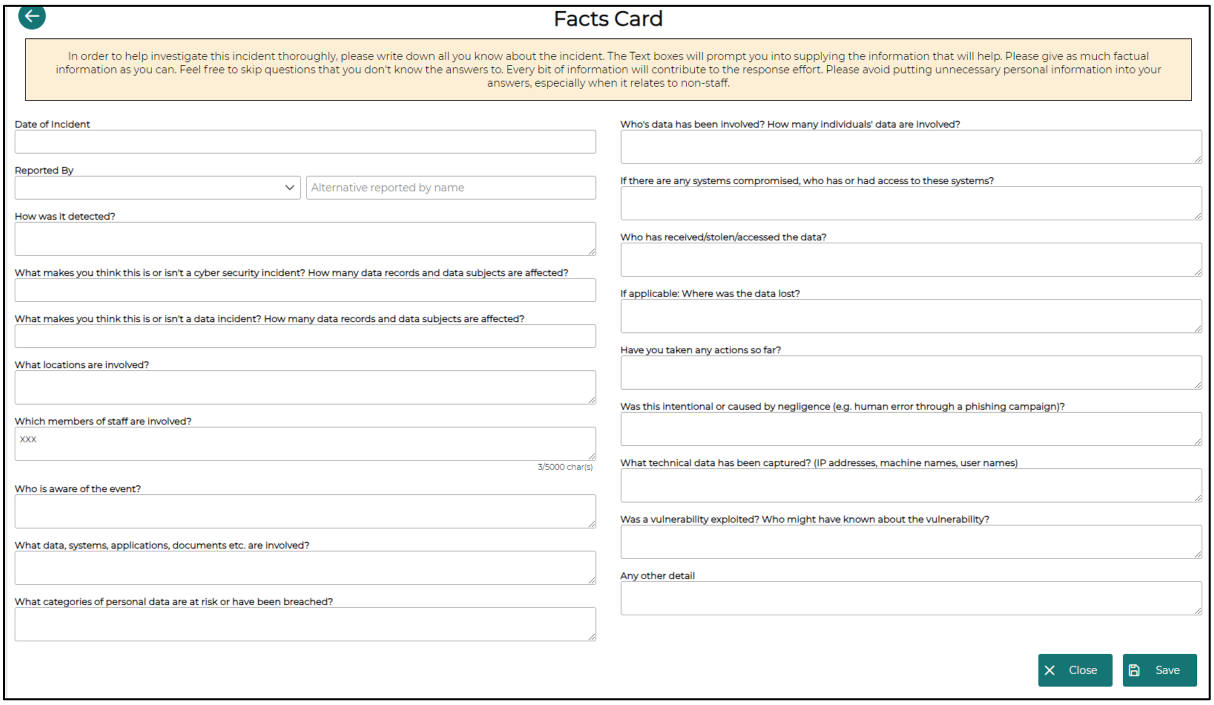
Description – Describe what has happened with regards to the incident however, please refrain from adding any personal identifiable information.

Type – You can select either a Breach, a Cyber Incident or both depending on the type of Incident which you are raising. This can be left blank if you are unsure at this point.

The incident type ‘Drill’ is so schools can run through a test scenario for an Incident.

Attach Document – An option has been provided for you to attach a document if required.

Once the Incident has been created you will be shown the “**Facts Card**” for you to fill in, to the best of your abilities, to provide as much information as you can regarding the Incident.



Facts Card

In order to help investigate this incident thoroughly, please write down all you know about the incident. The Text boxes will prompt you into supplying the information that will help. Please give as much factual information as you can. Feel free to skip questions that you don't know the answers to. Every bit of information will contribute to the response effort. Please avoid putting unnecessary personal information into your answers, especially when it relates to non-staff.

Date of Incident

Reported By

Alternative reported by name

How was it detected?

What makes you think this is or isn't a cyber security incident? How many data records and data subjects are affected?

What makes you think this is or isn't a data incident? How many data records and data subjects are affected?

What locations are involved?

Which members of staff are involved?

xxx

3/5000 char(s)

Who is aware of the event?

What data, systems, applications, documents etc. are involved?

What categories of personal data are at risk or have been breached?

Who's data has been involved? How many individuals' data are involved?

If there are any systems compromised, who has or had access to these systems?

Who has received/stolen/accessed the data?

If applicable: Where was the data lost?

Have you taken any actions so far?

Was this intentional or caused by negligence (e.g. human error through a phishing campaign)?

What technical data has been captured? (IP addresses, machine names, user names)

Was a vulnerability exploited? Who might have known about the vulnerability?

Any other detail

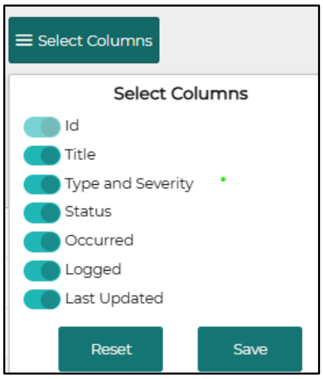
The purpose of the Facts Card is to provide as much information as you can as the raiser of the incident so that the appropriate members of staff can use that information in dealing with the incident.

Fill in as much information as you can and then click “**Save**” if you have made changes or “**Close**” if you simply wish to skip this page at this moment in time. You will be able to come back to the Facts Card later in the process if you choose to.

Updating an Incident

In order to update an incident, simply navigate to the Incident Log page via the navigation menu down the left-hand side of the portal and then click on the Pencil Icon for the Incident which you would like to update.

You can choose the columns that you want to see with Select Columns button



Select Columns

Id

Title

Type and Severity

Status

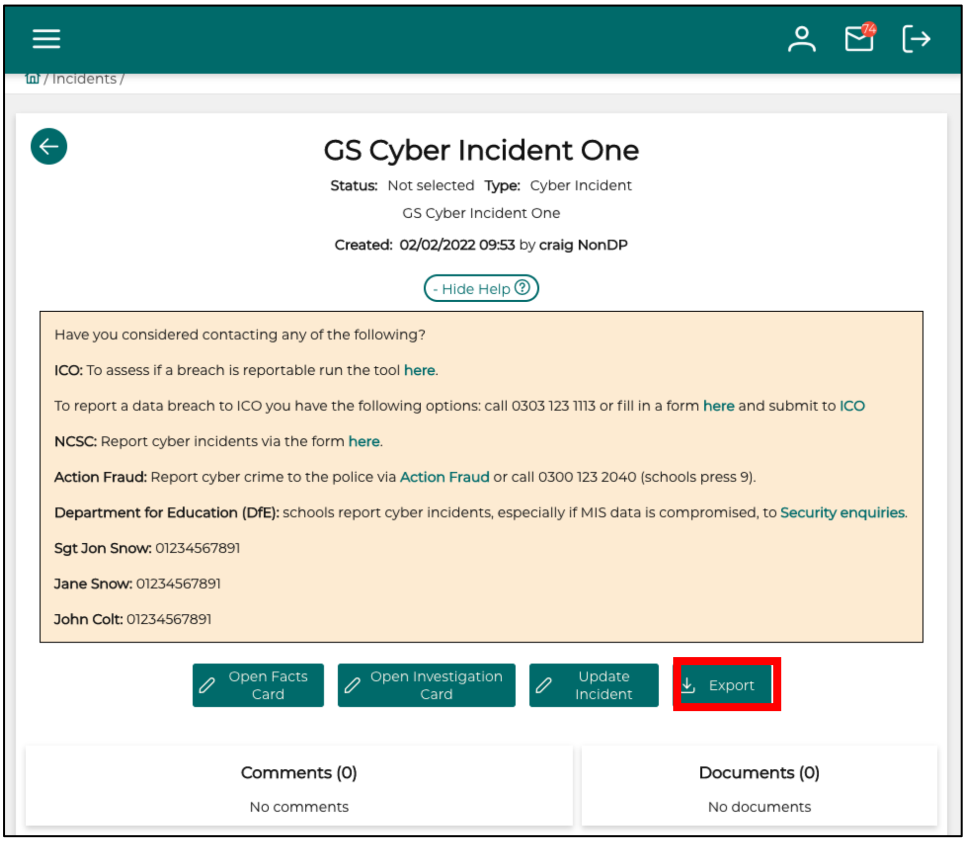
Occurred

Logged

Last Updated

Note: If no information has been provided on the Facts Card for your Incident at the time when it was raised, you will be prompted to provide any of the required information. You can either update the Facts Card and save your changes via the “**Save**” button or click “**Close**” to not make any changes and you will be taken to the Incident.

To update the incident, click on “**Update Incident**”.



GS Cyber Incident One

Status: Not selected **Type:** Cyber Incident

GS Cyber Incident One

Created: 02/02/2022 09:53 by **craig NonDP**

Have you considered contacting any of the following?

ICO: To assess if a breach is reportable run the tool here.

To report a data breach to ICO you have the following options: call 0303 123 1113 or fill in a form here and submit to ICO

NCSC: Report cyber incidents via the form here.

Action Fraud: Report cyber crime to the police via Action Fraud or call 0300 123 2040 (schools press 9).

Department for Education (DfE): schools report cyber incidents, especially if MIS data is compromised, to Security enquiries.

Sgt Jon Snow: 01234567891

Jane Snow: 01234567891

John Colt: 01234567891

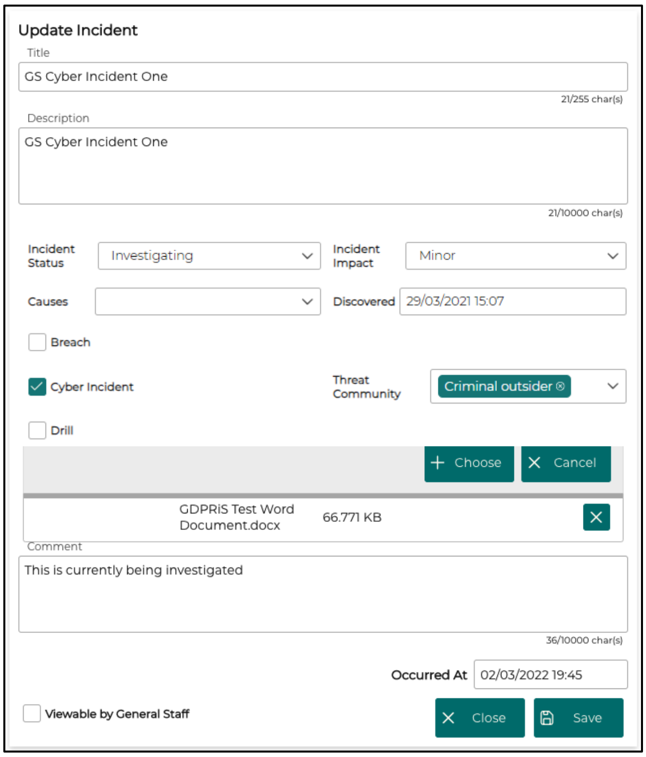
Comments (0)

No comments

Documents (0)

No documents

When you open the Update Incident window you will be provided with various options to update your incident. See screen shot for example:



Update Incident

Title: GS Cyber Incident One (21/255 char(s))

Description: GS Cyber Incident One (21/10000 char(s))

Incident Status: Investigating

Incident Impact: Minor

Causes:

Discovered: 29/03/2021 15:07

□ Breach

☑ Cyber Incident

Threat Community: Criminal outsider ⊗

□ Drill

GDPRiS Test Word Document.docx 66.771 KB

Comment: This is currently being investigated (36/10000 char(s))

Occurred At: 02/03/2022 19:45

□ Viewable by General Staff

Incident Status – The status is simply to provide a stage in its life-cycle which the Incident is currently in at the time.

Incident Impact – This is to show how severe the incident may impact the school

Cause – This is a long list of multiple selections to choose what contributed to or caused the incident. Please see Page 15 for explanation of causes

Discovered – When the incident came to the attention of a member of staff

Breach – This is a tick box to identify that the incident is a data breach and needs to be processed in such a way.

Cyber – This is a tick box to identify that the incident is a cyber security incident and needs to be processed in such a way. Note that many breaches are also cyber incidents. An example is, ransomware wipes (personal) data on a laptop and there is no backup, then this is a breach (data lost) but *also* a cyber security incident (ransomware attack).

Drill - This is a tick box to identify that the incident is a so schools can run through a test scenario for an Incident.

Breach Decision – This is to document your determination of whether the data breach is reportable. This was formally the breach "**Type**". (This option is only visible if "**Breach**" tick box is selected)

Breach Reporting Obligations Met – This tick box is to show that all data breach reporting activities have occurred for example, contacting ICO. (This option is only visible if "**Breach**" tick box is selected)

Threat Community – This is a multiple selection list showing who might be responsible for the incident happening.

Comment – When updating an incident, a comment is always required. Use this to document your justification for status changes.

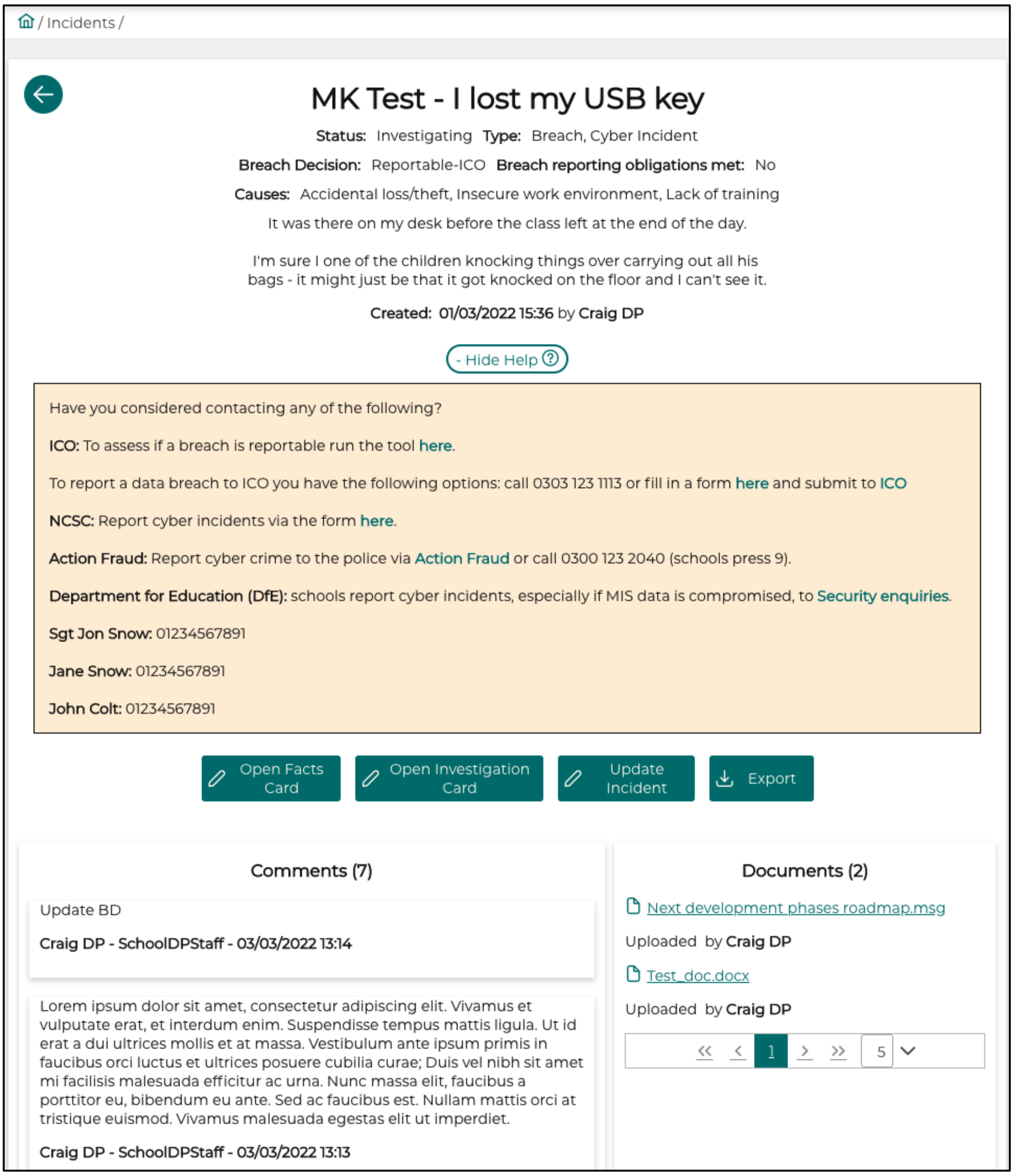
Attachment – This provides the functionality for you to upload a document regarding the incident.

Viewable by General Staff – This is a tick box so that if the incident was raised by a General Staff user type, that user would see the update and comment which is in the update.

If this is not selected, the General Staff user who raised the incident would not see the update.

This option will only be visible if the incident was raised by a General Staff user type.

In the screen shot below, you will be able to see an updated incident with comments, an attached document and the breach decision updated.



MK Test - I lost my USB key

Status: Investigating **Type:** Breach, Cyber Incident

Breach Decision: Reportable-ICO **Breach reporting obligations met:** No

Causes: Accidental loss/theft, Insecure work environment, Lack of training

It was there on my desk before the class left at the end of the day.

I'm sure I one of the children knocking things over carrying out all his bags - it might just be that it got knocked on the floor and I can't see it.

Created: 01/03/2022 15:36 by **Craig DP**

Have you considered contacting any of the following?

ICO: To assess if a breach is reportable run the tool here.

To report a data breach to ICO you have the following options: call 0303 123 1113 or fill in a form here and submit to ICO

NCSC: Report cyber incidents via the form here.

Action Fraud: Report cyber crime to the police via Action Fraud or call 0300 123 2040 (schools press 9).

Department for Education (DfE): schools report cyber incidents, especially if MIS data is compromised, to Security enquiries.

Sgt Jon Snow: 01234567891

Jane Snow: 01234567891

John Colt: 01234567891

Comments (7)

Update BD

Craig DP - SchoolDPStaff - 03/03/2022 13:14

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus et vulputate erat, et interdum enim. Suspendisse tempus mattis ligula. Ut id erat a dui ultrices mollis et at massa. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia curae; Duis vel nibh sit amet mi facilisis malesuada efficitur ac urna. Nunc massa elit, faucibus a porttitor eu, bibendum eu ante. Sed ac faucibus est. Nullam mattis orci at tristique euismod. Vivamus malesuada egestas elit ut imperdiet.

Craig DP - SchoolDPStaff - 03/03/2022 13:13

Documents (2)

Next development phases roadmap.msg

Uploaded by **Craig DP**

Test_doc.docx

Uploaded by **Craig DP**

Facts Card

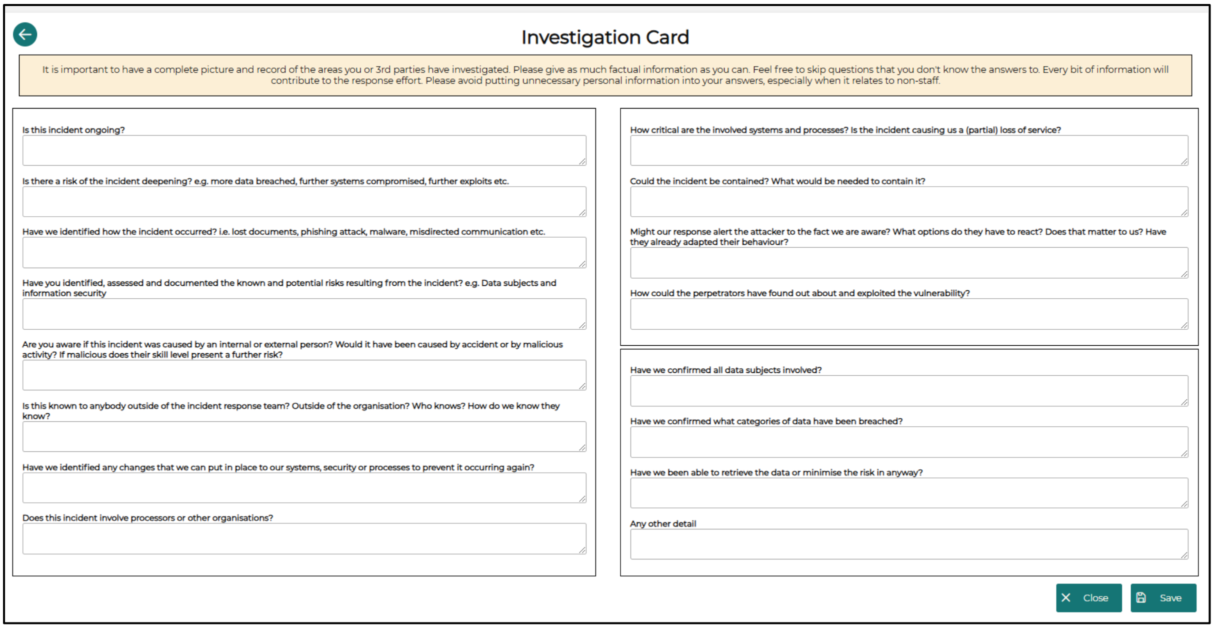
As previously described, the Facts Card is for information to be provided from the user who created the incident providing as much information as they can. The Facts Card can be accessed by navigating into the Incident and clicking on "**Open Facts Card**". This can be updated at any point of the incident life cycle.

State if this is a data breach and why you think that it is.

What locations are involved?

Investigation Card

There is a separate Investigation Card for the users who are investigating and resolving the incident in question. The Investigation Card can be accessed by navigating into the Incident and clicking on “**Open Investigation Card**”. This can be updated at any point of the incident life cycle.



Investigation Card

It is important to have a complete picture and record of the areas you or 3rd parties have investigated. Please give as much factual information as you can. Feel free to skip questions that you don't know the answers to. Every bit of information will contribute to the response effort. Please avoid putting unnecessary personal information into your answers, especially when it relates to non-staff.

Is this incident ongoing?

Is there a risk of the incident deepening? e.g. more data breached, further systems compromised, further exploits etc.

Have we identified how the incident occurred? i.e. lost documents, phishing attack, malware, misdirected communication etc.

Have you identified, assessed and documented the known and potential risks resulting from the incident? e.g. Data subjects and information security

Are you aware if this incident was caused by an internal or external person? Would it have been caused by accident or by malicious activity? If malicious does their skill level present a further risk?

Is this known to anybody outside of the incident response team? Outside of the organisation? Who knows? How do we know they know?

Have we identified any changes that we can put in place to our systems, security or processes to prevent it occurring again?

Does this incident involve processors or other organisations?

How critical are the involved systems and processes? Is the incident causing us a (partial) loss of service?

Could the incident be contained? What would be needed to contain it?

Might our response alert the attacker to the fact we are aware? What options do they have to react? Does that matter to us? Have they already adapted their behaviour?

How could the perpetrators have found out about and exploited the vulnerability?

Have we confirmed all data subjects involved?

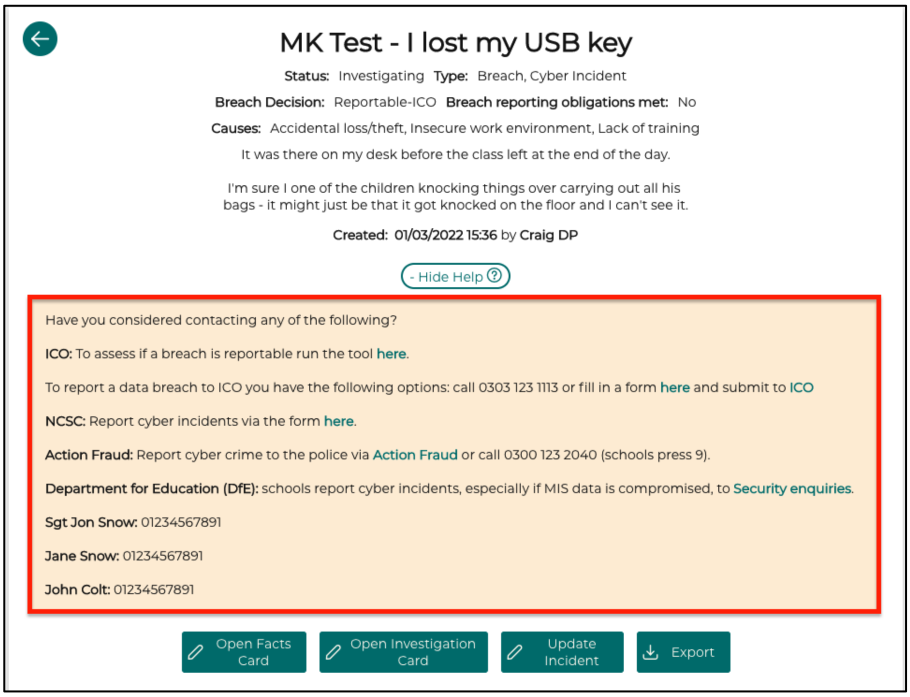
Have we confirmed what categories of data have been breached?

Have we been able to retrieve the data or minimise the risk in anyway?

Any other detail

Helpful Information

In the different parts of the Incident Management Tool are sections of text to provide helpful information on how to fill in the relevant section you are in or what to do etc. Please refer to these if you need to.



MK Test - I lost my USB key

Status: Investigating **Type:** Breach, Cyber Incident

Breach Decision: Reportable-ICO **Breach reporting obligations met:** No

Causes: Accidental loss/theft, Insecure work environment, Lack of training

It was there on my desk before the class left at the end of the day.

I'm sure I one of the children knocking things over carrying out all his bags - it might just be that it got knocked on the floor and I can't see it.

Created: 01/03/2022 15:36 by **Craig DP**

Have you considered contacting any of the following?

ICO: To assess if a breach is reportable run the tool here.

To report a data breach to ICO you have the following options: call 0303 123 1113 or fill in a form here and submit to ICO

NCSC: Report cyber incidents via the form here.

Action Fraud: Report cyber crime to the police via Action Fraud or call 0300 123 2040 (schools press 9).

Department for Education (DfE): schools report cyber incidents, especially if MIS data is compromised, to Security enquiries.

Sgt Jon Snow: 01234567891

Jane Snow: 01234567891

John Colt: 01234567891

Export

We have provided the means for you to export the information from your incident to a Word document, so that it can be provided to users outside of your GDPRiS portal. Navigate to your incident which you would like to export, click on “Export”. (This will open a popup window)

You will be able to save the report to a location of your choosing.

The report provides the following information from your incident:

Incident Summary:

Organisation Name
Incident Number
Date when the incident was logged
Incident Title
Incident Description
Status
Incident Impact
Causes
Incident Type
Date when the Incident was discovered
Breach Decision
Breach Obligations Met
Comments
Answers from the Facts Card
Answers from the Investigation Card

Explanation of Causes

(Distributed) Denial of Service	Explanation
Accidental loss/theft	Most typically this is the loss or theft of either a device such as a laptop or a mobile phone, or of hardcopy data (e.g. paper files). Even if the data is encrypted, the event is still an incident, albeit probably less severe.
Adversary-in-the-Middle	Also called man-in-the-middle attack: this is where an attacker intercepts traffic and is able to either read, or even alter its contents.
Brute force	If an attacker has access to a data repository (e.g. via a login form), they can try to make thousands of attempts at guessing the password. Lists of common passwords and some reconnaissance on their victims help with this type of attack.
Data exfiltration	This is a type of data loss event, where you discover that data has intentionally ro accidentally been leaked to outside the confines of your control and to unauthorised recipients.
Excessive data held	If you hold too much data, or you hold data for longer than is necessary to meet the purpose of your processing activity, this is a breach of your data protection policy and a breach of the law.
Hacking (session hijacking, injection attacks, keyloggers, ..)	A broad class of events, where malicious individuals attempt to misuse your information resources in an attempt to compromise them. The skill level of hackers, aswell as their motivation can vary widely (e.g. protest, personal gain, thrill). The methods and the results of hacking also vary widely.
Inadequate contract	If processing activity is not covered by a contract, that gives both parties of the contract sufficient protection, or the data subjects.
Inadequate policy	Policy can refer to a written document, instructing your workforce how to behave. It can also refer to a technical control that enforces certain behaviour.
Inappropriate disposal	After the period of usefulness ends for data it needs to be disposed of. Disposal is inappropriate if the data can be recovered.
Inappropriate handling	Inappropriate handling usually refers to a violation of data safeguards. Examples could be: unauthorised members of staff or other bodies were involved, careless sharing or diclosing of documents.
Insecure work environment	Where the work environment is such, that unauthorised individuals can easily get access to information, e.g. by eavesdropping on conversations or by overlooking computer screens. Or indeed, physical measures such as doors or locks are not sufficiently strong.

Lack of training	Lack of awareness and skill often result in incidents
Malware or Ransomware	Malware and a special type of malware called Ransomware are very often spread via emails, and unsuspecting members of staff will infect first their machine and then their co-workers' machines. Malware infections are at least disruptive, but can easily cause severe incidents and data breaches.
Misconfiguration	Misconfigured computers are open to a wide variety of forms of attacks. It is good practice to apply consistent and strong security settings to all computers.
Misdirected communication	One of the most common forms of data breach is when email accidentally includes inintended recipients.
Negligence	Staff who are not fully aware of or willingly choose to ignore policy.
No/weak encryption	Encryption and good key management are good ways to protect information. The absense of either puts data at risk of breach.
Phishing	Phishing emails - cleverly worded emails to prompt recipients into disclosing secrets or making payments.
Processing not in line with rights	Under data protection law, data subjects enjoy a number of rights. If an organisation is not able or willing to satisfy those rights, they are breaking the law.
Social engineering	Malicious activities using human interaction, usually employing psychological manipulation.
Supply chain attack (vendor compromise)	An attack on an organisation by first attacking and compromising less secure entities in the supply chain.
Trojan	A Trojan is malware, packaged and installed as part of legitimate looking software.
Unintended disclosure of sensitive data	Sensitive data (esp also personal data) that get into the hands of unauthorised recipients.
Unlawful processing	Processing of personal data, that is taking place either without or with dubious lawful basis, or otherwise contravenes the GDPR.
Unpatched systems	Malware and hackers often go after unpatched systems.
Unsolicited marketing	Sending marketing information without the necessary consent (opt-in) according to Privacy and Electroniic Communications Regulation (PECR).
Violation of Acceptable Use Policy (AUP)	The Acceptable Use Policy - if defined - instructs your staff what they can and can't do with the data and computer systems of your school.
Weak/Compromised credentials	Hackers make attempts at guessing weak passwords. Even in the absense of an actual compromise, weak credentials (e.g. the use of shared or common passwords) is a security incident.

Contact the Customer Success Team

Office hours

Mon-Thurs:	09:00 - 16:30 GMT
Fri:	09:00 – 15:30 GMT

If you require assistance regarding any section of this help guide, please do not hesitate to contact us via one of the following methods:

Tel: 02039 610 110

Mail: support@gdpris.co.uk