AIR-NET

Breach Reporting

What is a breach?

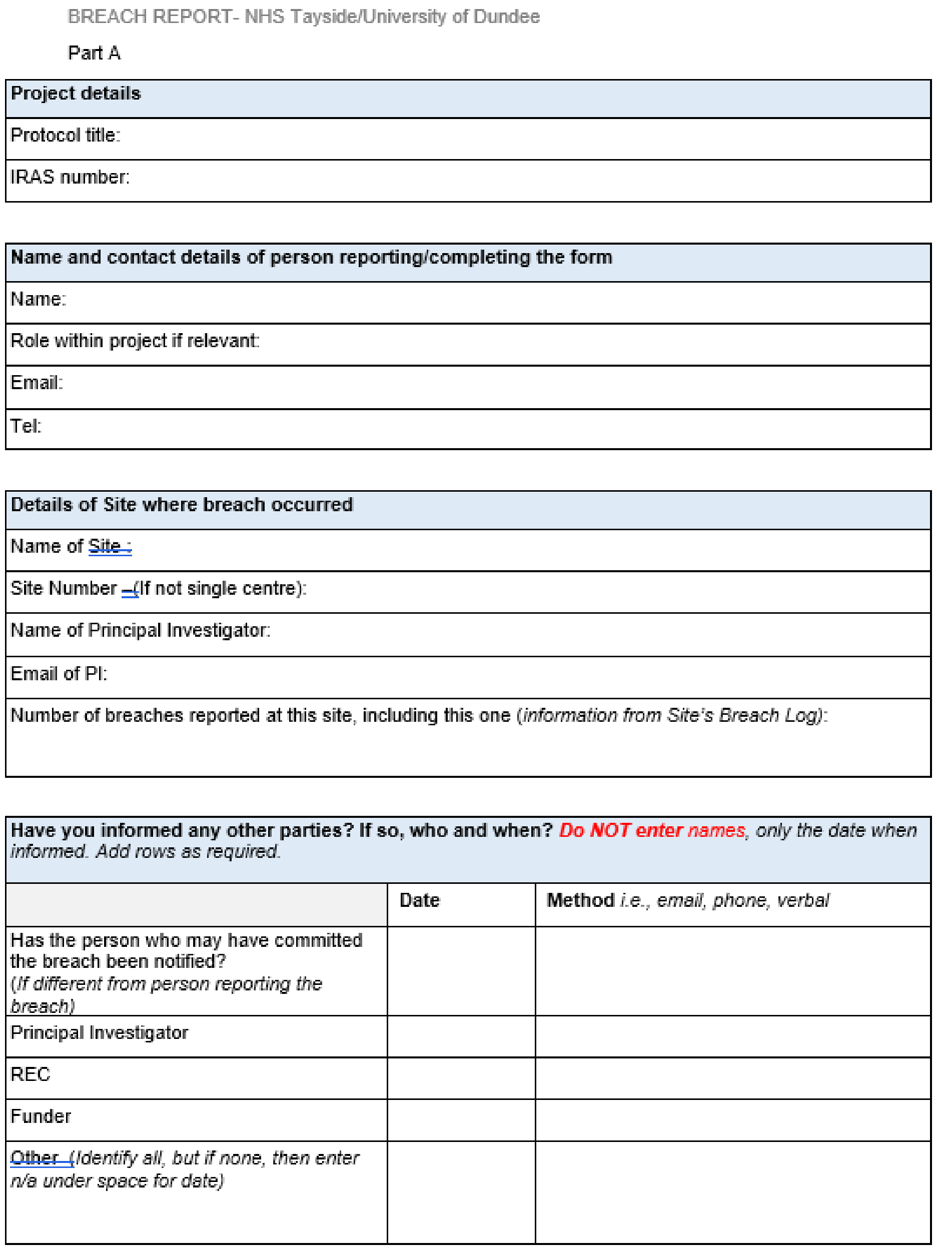
- Any departure from:
  - Approved Protocol
  - Conditions of approvals
  - Principles of GCP
  - Written procedures (SOPs)
  - Regulatory requirements
  - Insurance cover
  - Contractual obligations
  - Confidentiality and GDPR
- Our Sponsor does not recognise deviations – all deviations should be classified as breaches and reported.

Breach reporting

- Breach reporting is the responsibility of the site team
- Breach report is made directly to the Sponsor
- The breach reporting form must be downloaded from TASC website each time it is required, to ensure you are using a correct version
- The form can be found under TASC SOP59:

https://www.dundee.ac.uk/tasc/policies-sops-templates/study-progress

- Email breach report form to tascpotentialbreach@dundee.ac.uk & copy in airnet-tm@dundee.ac.uk
- Ensure correct breach numbering is used by referring to the site Breach Log
- The Sponsor will close and categorise the breach form and send a copy back to the site team
- Every breach must be documented on the Breach Log in the site file
- Each closed breach report must be filed in the ISF



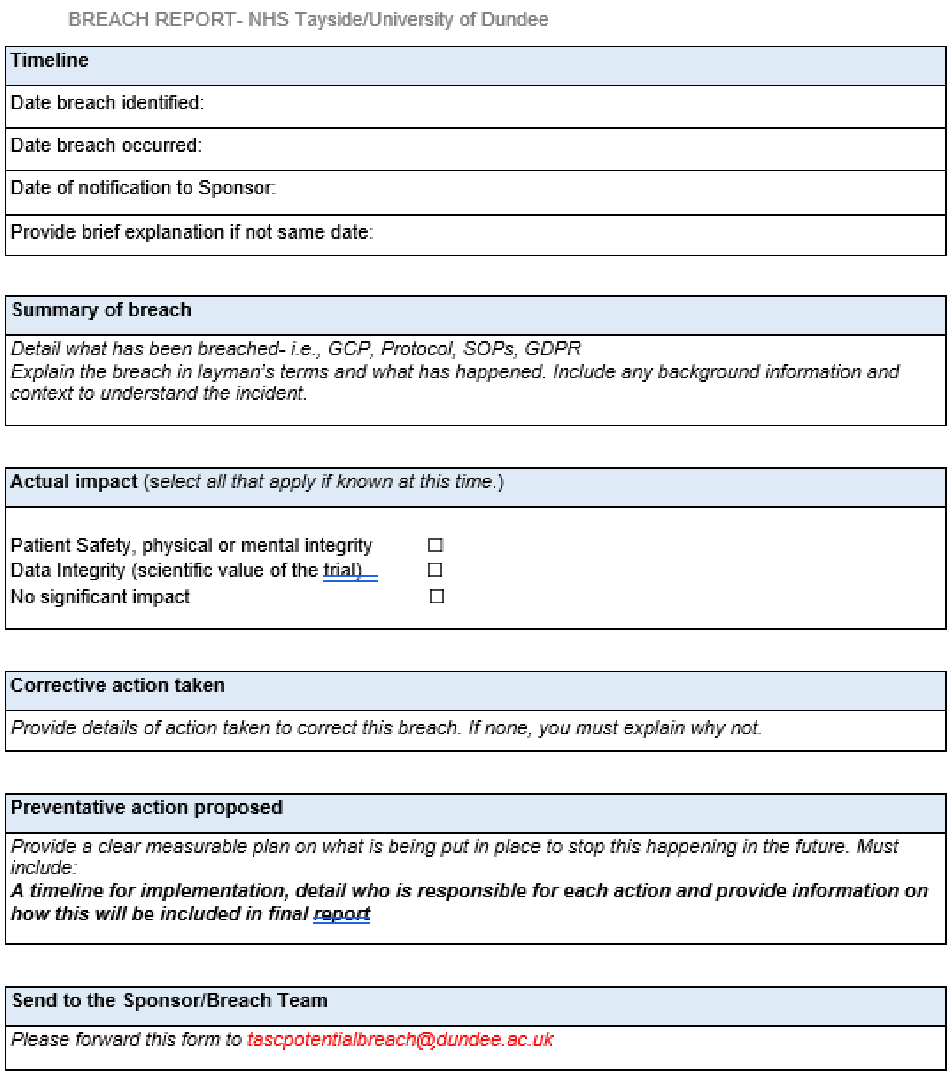
Part A

Project details
Protocol title:
IRAS number:

Name and contact details of person reporting/completing the form
Name:
Role within project if relevant:
Email:
Tel:

Details of Site where breach occurred
Name of Site :
Site Number –(If not single centre):
Name of Principal Investigator:
Email of PI:
Number of breaches reported at this site, including this one (*information from Site's Breach Log*):

Have you informed any other parties? If so, who and when? *Do NOT enter names,* *only the date when informed. Add rows as required.*		
	Date	**Method** *i.e., email, phone, verbal*
Has the person who may have committed the breach been notified? *(If different from person reporting the breach)*		
Principal Investigator		
REC		
Funder		
Other (*Identify all, but if none, then enter n/a under space for date)*		



Timeline
Date breach identified:
Date breach occurred:
Date of notification to Sponsor:
Provide brief explanation if not same date:

Summary of breach
Detail what has been breached- i.e., GCP, Protocol, SOPs, GDPR *Explain the breach in layman's terms and what has happened. Include any background information and context to understand the incident.*

Actual impact (*select all that apply if known at this time.*)	
Patient Safety, physical or mental integrity	□
Data Integrity (scientific value of the trial)	□
No significant impact	□

Corrective action taken
Provide details of action taken to correct this breach. If none, you must explain why not.

Preventative action proposed
Provide a clear measurable plan on what is being put in place to stop this happening in the future. Must include: ***A timeline for implementation, detail who is responsible for each action and provide information on how this will be included in final report***

Send to the Sponsor/Breach Team
Please forward this form to tascpotentialbreach@dundee.ac.uk

Corrective And Preventive Action (CAPA)

- **Corrective**
  - What did you do to fix it?

- **Preventive**
  - Preventive action is to stop the problem from happening again, e.g checklist, training, new SOP, etc.

Are breaches always serious?

No.

- The majority are technical breaches that do not result in harm to the trial participants or significantly affect the scientific value of the reported results
- But…several non-serious breaches can become one Serious Breach as collectively they do have a detrimental impact
- Therefore, ALL must be reported to Sponsor and documented on the Breach Log
- If you are unsure, report anyway