University of
St Andrews

University cyber incident and data breach management procedure

Document type	**Procedure**
Scope (applies to)	All staff
Applicability date	05/02/2020
Review / Expiry date	05/02/2023
Approved date	04/02/2020
Approver	Vice-Principal
Document owner	Head of Info Assurance & Governance
School / unit	Office of the Principal
Document status	Published
Information classification	Public
Equality impact assessment	None
Key terms	Information governance and management/Information security
Purpose	Protocol for managing suspected data/personal data breach

Version number	Purpose / changes	Document status	Author of changes, role and school / unit	Date
1.0	Procedure incorporates previously approved procedures for data and personal data breaches	Approved		

1. Introduction

Purpose of this document

This procedure sets out in broadly chronological order the steps to be taken in order to manage suspected or actual data breaches, whether they involve personal data (as defined by the General Data Protection Regulation ("the GDPR") and the Data Protection Act 2018 ("the DPA 2018")) or otherwise. It should be noted that some sections of the plan will in practice run concurrently; the Institution must retain the ability to be flexible and responsive on a case by case basis.

This plan provides a framework from which the University can:

- Meet its legal and moral duty to notify the ICO and to inform individuals, where appropriate to do so, of any notifiable personal data breach;
- Initiate a timely and appropriate response to contain and prevent further loss of and/or unauthorised exposure of data;
- Learn promptly and positively from instances of data loss, whether Personal Data or otherwise, to strengthen the organisational and technical measures that are in place to protect the confidentiality and availability of data;
- Establish an audit trail to enable the University to demonstrate to the supervisory authority, and any affected persons, how it has evaluated and responded to any data breach; and
- Ensure that adequate records are created and maintained, to meet legislative requirements.

Relationship to other protocols and plans

IMPORTANT Within some areas of the University's operation, specific data breach management plans are available for data processing activities that are fully understood. A notable example is the breach management plan for entry qualification data loss during the Universities and Colleges Admissions Service embargo periods. Where a specific protocol exists, that protocol should be followed.

This procedure complements the University Crisis Management Plan in relation to escalation to Principal's Office ("the PO") (Section 3) but otherwise this procedure supersedes the Crisis Management Plan.

Review of this document

The procedure will be reviewed at regular intervals, as recorded on the cover sheet. Earlier review may be triggered by: changes to relevant legislation and/or guidance issued by the UK Information Commissioner ("the ICO") or by the European Data Protection Board; changes to University policy or procedures concerned with protection of personal data; changes to University policy or procedures related to CSIRT and cyber security, or by governmental stakeholders associated with those processes; and any Incident debrief which suggests that procedural review would be beneficial.

Enquiries about this procedure should be directed to Head of Information Assurance and Governance (Chris Milne) or University IT Security Officer (Patrick Green).

Section 1: Initial Notification and Incident Controller Nomination

If a data breach has occurred or is suspected, then this should be notified immediately to:

- IT Services Desk – 01334 463333, or
- St Andrews CSIRT – 01334 462759 (stacsirt@st-andrews.ac.uk), or
- Information Assurance and Governance Team – 01334 464010 / 01334 462779 (dataprot@st-andrews.ac.uk)
- If outwith normal business hours, contact IT Services Out of Hours, 01334 462780

First person notified should contact either The Head of Information Assurance and Governance (Chris Milne) or IT Security Officer (Patrick Green).

- Chris Milne and Patrick Green will liaise and nominate whichever of themselves is the most appropriate Incident Controller relative to the type of Incident.
- In the event only one of Chris Milne or Patrick Green is contactable, that one automatically takes the role of Incident Controller.
- Alternate Incident Controllers, in the absence of both Chris Milne and Patrick Green, are the Chief Information Officer (Steve Watt) or the Depute Chief Information Officer (Dean Drew).
- If Chris Milne is not contactable, then any breach involving Personal Data is notified to the Freedom of Information Officer (June Weir) by the nominated Incident Controller.

The Incident Controller's role is to co-ordinate the initial response and secure the necessary resource to manage the incident with support of colleagues and PO.

- In particular, the Incident Controller will ensure initial triage and evaluation of the incident in line with section 2 (Incident Triage and Early Risk Evaluation) and then proceed to Section 3 (Incident Management Team and Escalation) ("the IMT").

2. Section 2 – Incident Triage and Early Risk Evaluation

Once the incident has been logged, the Incident Controller will classify the nature of the breach using the standard categories;

https://itservices.wp.st-andrews.ac.uk/files/2020/01/Standard_Categories_for_Incident_Response_2.1-1.pdf

External investigation	Internal investigation	APT
Malicious code	Denial of Service	Social
Copyright infringement	Unauthorised access	Threat/Extortion/Blackmail

Early evaluation of the Incident

The Incident Controller will also make an early risk-based evaluation of the incident, using RAG Triage Spreadsheet for Risk Evaluation (available to Patrick Green, Sam Foster, Chris Milne and on Crisis and Continuity SharePoint site).

Assess the type of information and link to GDPR

Evaluate the type of information that is stored on the system, using the University Information Classification system: Public; Internal; Confidential; Strictly Confidential
(available from the policy zone, https://www.st-andrews.ac.uk/policy/index.php).

If the incident involves information/data classified as Internal, Confidential or Strictly Confidential as per the University Information Classification scheme, then the risk evaluation must also determine if any Personal Data (Appendix A) is involved.

The ICO only requires to be notified of a personal data breach where it [the breach] "…is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage." [1]

If the loss involves personal data (where the University is the controller, i.e. responsible for), then we must classify the Breach using Appendix B. All personal data breaches classified as High and Medium must be reported to the ICO within 72 hours of the University becoming aware of the breach in line with Section 5 of this procedure. A data controller [the University] is not required to notify where it has been assessed that a breach is unlikely to result in any risk to the rights and freedoms of individuals affected by the breach.[2]

Chris Milne, is to be involved in decisions concerning the classification of a personal data breach and breach notification or in his absence, June Weir or the University Chief Legal Officer[3].

[1] ICO, Breach notification, available from: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/breach-notification/, accessed 13 September 2017.
[2] GDPR, Recital 85.
[3] GDPR, Article 39, paragraph 1(d).

Section 3: Incident Management Team (IMT) and Escalation

Calling out the IMT

Incident Controller to trigger core and non-core IMTs, broadly in line with appraisal from our Section 2 initial risk evaluation.

- The Incident Controller is not constrained by guidance below and can escalate the outcome from that indicated by the Heat Map where they feel that is appropriate.
- The Incident Controller is empowered to take all actions required to accomplish their role.
- For Critical and Major incidents, where the action may have a significant adverse effect on other University activities, this will be escalated to Vice-Principal, Governance ("VP Gov") (Alastair Merrill), failing which Quaestor and Factor (Derek Watson) or Master (Lorna Milne) in line with corporate Crisis Management Plan.

Heat Map Outcome	Notifications by Incident Controller
Critical – major threat to the business and/or external parties	Notify ALL core IMT primary contacts (or deputies). Also notify non-core IMT members to the extent the Incident Controller deems appropriate at the time.
Red – potentially major incident	Notify ALL core IMT primary contacts (or deputies) Also notify non-core IMT members to the extent the Incident Controller deems appropriate at the time.
Amber – serious but manageable	Notify ALL core IMT primary contacts (or deputies). This is for information only, unless the assessment should deteriorate, or their specific expertise is requested. Also notify whichever non-core IMT members the Incident Controller deems appropriate.
Green – localised event	Incident Controller manages and delegates the Incident in line with Business as Usual (BAU) procedures.

The core Incident Management Team and roles

Primary Contact	Deputy	Role
Chris Milne (*)	Patrick Green	GDPR – Incident Controller and Incident log
Patrick Green	Chris Milne (*)	Cyber – Incident Controller and Incident log
Steve Watt	Dean Drew	IT - resource, solutions, mitigation, workarounds
Roy Drummond	Mike Gettinby	Legal
Niall Scott	Emma Shea	Comms – PR, media, stakeholder liaison
VP Gov	Quaestor / Master	Responsible for escalation to PO

(*) if Chris Milne is not available then also notify June Weir, Information Assurance and Governance Officer from non-core IMT, where there is Personal Data exposure

The non-core Incident Management Team and roles
These people are notified when the incident may impact their business area

Name	Deputy	Role
June Weir	-	Personal Data – deputy to Chris Milne
Sam Foster	-	Cyber security – deputy to Patrick Green
Tom Brown	Helen Reddy	Research and Innovation
Marie-Noel Earley	Helen Boyd	Registry
Lara Meischke	Rita Unsworth	Student Services
Helen Mackie	Andy Edmonston	Estates – security and theft or malicious damage
Brian Kennedy	Ali Mconnell	Insurance
Laura Knox	Moira Sinclair	Timetabling
Calli Hopkinson	Allyson McCrossan	Finance
Mairi Stewart	Louise Nixon	HR

VP Gov (deputised by Quaestor / VP Education) will escalate Red and Amber Incidents to the Principal, Fiona Thompson and Niall Scott, in line with the University Crisis Management Plan.

- Role of PO contacts is by default that of assurance, governance and gatekeeper for suitable resource to manage the Incident, where requested by the Incident Management Team

For Critical Incidents, the Incident Controller will be responsible for ensuring completion of the reporting form in Appendix B and escalating the Incident in compliance with the current version of the Scottish Public Sector Cyber Incident Central Notification and Co-ordination Policy, issued by the Scottish Government.

The Incident Controller should follow this up by contacting at least one of: The Duty Officer at the Scottish Government Cyber Resilience Unit (CRU) 0300 244 4000; Police Scotland tel. 101 and ask for Cyber unit On Call Officer; SGOR 07623 909978 (pager) and ask for SGOR Duty Officer.

The triggers for notification to this audience are that an Incident will;

- Have potential to disrupt (critical aspects of) the continued operation of the organisation or delivery of public services, and/or
- Carries a likelihood that other organisations may experience a similar attack or that the Incident could spread to them, and/or
- Could have a negative impact on the reputation of the Scottish public sector or Scottish Government, and/or
- Carries the likelihood of Scottish Parliament or national media interest.
- In addition, OSCR (Scottish Charity Regulator) and SFC (Scottish Funding Council)

3. Section 4 – Breach Containment and Isolation

Responsibility and resource

StACSIRT will take the lead on investigating the source and cause of the breach.

It may be judged necessary to take immediate action to contain a suspected or actual breach. Such actions could include removal of devices from the University network, suspension of ICT services. Where this plan is put into effect, the instructions of the IMT are to be followed. If there is any dispute VP Gov, Quaestor or Master will be the final arbiter, unless other arrangements have been put in place and approved by a member of the Principal's Office.

VP Gov, Quaestor or Master to provide the resources necessary to isolate and contain the breach, where additional resource beyond that which is normally available to the Chief Information Officer or the Head of Information Assurance and Governance is required.

Create an Incident Log

The Incident Controller must ensure an incident log is opened and maintained to record our decisions and response to the Incident. If the task is delegated, the Incident Controller remains responsible for quality control of that log. The log will be backed-up frequently during the incident and held for six years after the last actions relating to the breach have been concluded. The log will record:

- Facts relating to the breach, including first notification time / date and effects of the breach;
- Initial breach risk evaluation and rationale for this along with any remedial actions agreed;
- Follow-up breach risk evaluation, and supporting or contextual information;
- Feedback from stakeholders;
- All actions considered by StACSIRT along with rationale for those which have been either implemented or rejected; and
- Outcome from actions implemented and tracking mechanism to ensure completion and feedback on efficacy of the action.

The University Information Assurance and Governance function maintains a log for personal data breaches.

Considerations for StACSIRT, combined with Information Assurance may include

- Where is the data held (if relevant, was there a travel risk assessment).
- If relevant, what details did the UTREC application hold, with respect to encryption.
- What was the configuration of the system, where are the logs stored and what back-ups are available (if the back-ups are encrypted, is the decryption key available?).
- Establish who needs to be aware of the breach and inform them of what they must do, either targeted or through broad staff and student alerts.
- Preserve evidence to understand the breach and/or to allow for criminal investigations.
- Establish if external resource is required, for instance forensic analysis, or whether Police Scotland could advise on evidence preservation and management.
- Confirm with the Chris Milne, what measures are being implemented with regard to personal data, so that the University can meet its legal obligation to notify the ICO, within 72 hours of the breach having come to light, or within a phased notification period agreed with the ICO.
- Identify the potential source of the breach and agree the scope of investigation.
- Establish if we can trace, recover or remotely destroy or deny access to lost data.
- If data has been lost from a mobile device/handset etc. which is linked to University e-mail and/or remote services, for the device(s) to be locked and/or all data to be remotely wiped.

- Where data have been miscommunicated to a third party, take steps to secure the return of those data, involving the Chief Legal Officer, or deputy, where data has not been returned.
- Stop further processing of data to prevent additional losses.
- Implement IT disaster recovery plans where to do so does not expose the University to additional risk.
- Obtain contracts relative to any third-party providers involved.
- If a third-party provider is involved, ensure they liaise first and foremost with the University.
- What actions may individuals have to take to prevent any further risk to their privacy – do passwords require to be changed, do students/staff need to inform their bank that payment details have been compromised, does the University need to advise on how to prevent identify theft?
- Develop secondary communications to other stakeholders. NB it is normal practice to provide minimal information on the nature of the breach and its impact until the source and extent of a breach have been confirmed.
- Consider removing the system from the network or applying firewall / network blocks.
- Ensure that existing system auditing remains intact and has been operational. If auditing has been disabled (to cover someone's trail, for instance), restore it before proceeding.
- Consider changing passwords or locking credentials relative to all involved accounts, whether confirmed or suspected.
- Purging of emails.

Care must be taken to ensure that action does not make the situation worse. Specific actions can be discussed as part of the incident and will involve technical input to the IMT. If the business can withstand the risk, recovery should take place after the evaluation in order to prevent logs being overwritten or for issues to be found after recovery has been put in place, which would have changed the recovery process.

Further analysis will require other members of the incident response team, depending on the incident. Sources might include;

- School computing officer
- IT Services staff

4. Section 5 – Notification of a Personal Data Breach to the ICO

IMPORTANT The University, where it is responsible under data protection legislation for safeguarding personal data of individuals is required to formally notify the ICO, within 72 hours and without undue delay of it having become aware of a personal data breach, unless, after assessment, it can be demonstrated that the breach is unlikely to result in a risk to the rights and freedoms of the persons concerned.

In addition to notifying the ICO of a data breach, within 72 hours, where it has been assessed that the data breach is likely to result in a high risk of harm befalling the persons concerned, then those who are affected by the data breach must also be informed as to what has happened, and what steps/precautions, if any, should be taken to guard against harm arising, or to mitigate to reduce harm.

The University may not be required to inform individuals where a data breach has occurred; see **Exemptions from the obligation to notify**, below.

Within 72 hours, and without any undue delay, the Head of Information Assurance and Governance, deputised by the Information Assurance and Governance Officer, will present an assessment to VP Gov detailing whether a personal data breach is notifiable to the ICO, who in turn will make a final decision. This process will involve;

- Working with the IMT to establish the basic facts surrounding the breach and confirm the prior assessment as to whether a suspected breach does or does not involve personal data.
- Deciding with VP Gov (or alternate) whether the breach is reportable to the ICO
- Deciding with VP Gov (or alternate) whether to inform those affected by the breach
- Working with the IMT to determine what containment measures and forms of mitigation and/or recovery can be engaged, making all necessary requirements to do so
- Arranging for notification to be made to the ICO or where full notification to the ICO is not possible, a phased response is to be made within the 72 hour period.
- Securing resources as necessary to manage the breach
- Where we are required to do so, individuals affected are to be notified at the earliest opportunity of the breach, along with any actions to be taken by those individuals to minimise harm
- Recording the breach and maintain a record of all key events.

IMPORTANT Individuals are to be notified of a personal data breach where it is classified as either High or Medium, according to Appendix B.

Additional considerations to be discussed with the IMT include:

- Establish whether notification must be delayed relative to law enforcement priorities.
- Consider the University's response to any unauthorised information leaks (to the press or social media) concerning the breach, prior to formal notification to the ICO, by the University.
- Confirm the target audiences to be communicated with, beyond those with whom notification is a legal requirement.
- Establish the communications to be made with each target audience (priority should be to those who are likely to be exposed to the highest level of risk/damage resulting from the data loss; and
- Consider legal review of all communications prior to their issuance.
- Could urgent notification help the individuals concerned (e.g. changing of passwords)?
- Monitor traditional and social media for third-party reaction and reporting of the breach.
- Consider whether notification to Audit and Risk Committee is required from VP Gov.
- Determine whether insurers be notified.
- Establish whether call centre capability etc. may be required to deal with incoming enquiries.
- Consider impact on reputation and available remedies or mitigation.
- Align media message with any third-party service provider involved.

Data controllers [the University] are exempt from the obligation to notify individuals affected by a personal data breach where one or more of the following conditions are met:

- Technical security/protection measures are in place to ensure that the data are protected despite the breach e.g. where personal data are encrypted so that those data are unintelligible to any third-party who is not authorised to access those data [4].
- Subsequent actions taken have removed the risk to individuals or mitigated against this substantially[5] e.g. if a device has been lost and the content of that device has been remotely wiped or access to the device has been locked denying an unauthorised third-party access.
- Where a trusted person has accidentally received personal data and they have not acted on the materials which have incorrectly been made available to them.
- Issuing notification to those affected would involve a disproportionate effort[6]. In such cases alternative forms of notification will be required e.g. an advert in local/national media, notice on the University web site etc.

As a minimum, the information reported to the ICO must contain[7]:

- A description of the nature of the personal data breach including, if possible, the categories and approximate number of individuals [data subjects] and the categories and approximate number of records subject to the breach;
- The name and contact details of the University's Data Protection Officer or an alternative point of contact, from whom the ICO can source additional information; and
- A description of the measures which have been taken, including those which are intended to mitigate the possible adverse effects.

[4] GDPR, Article 34, paragraph 3(a).
[5] GDPR, Article 34, paragraph 3(b).
[6] GDPR, Article 34, paragraph 3(c).
[7] GDPR, Article 33, paragraph 3.

Form of the notification:

- The University will make use of templates/forms provided by the ICO, where available. Alternatively, a document, following the template available in Appendix C will be used.
- Content of the notification notice to the individuals [data subjects]
- Notification made to individuals must be given in clear and plain language, describe the nature of the breach and include the same information as that included in the notice issued to the ICO [8].
- Prior to issuance, VP Gov or their alternate, will approve the content of notifications.

[8] GDPR, Article 34, paragraph 2.

5. Section 6 – Detailed Investigation and Recovery

StACSIRT must undertake an urgent detailed investigation, building on the initial risk evaluation and containment measures. For Critical and Major incidents, the IMT can take the decision if an external service should be involved, for instance an Internal Auditor.

What happened?

- Describe the systems that were compromised.
- What data have been lost and/or exposed to an unauthorised third-party?
- What is the volume and sensitivity of the data loss?
- How many people and/or records are affected?
- Are any high-profile individuals involved?
- What were the methods employed that led to the data breach?
- Which accounts may have been utilised?
- What factors or failings may have contributed to the breach?
- Has the breach been contained, or might it be ongoing?

Risk assessment

- Potential for current or future harm to the University
- Potential for current or future harm to individuals
- Likely implications of the data breach including from compliance perspective
- Possible regulatory and contractual penalties
- Financial, operational and reputational repercussions, current and future
- Describe best- and worst-case scenarios with likelihoods

Recommendations

- Actions we should take to mitigate harm from this breach to the University or individuals
- Additional actions which may be necessary to further contain this data breach
- Any technical, behavioural or procedural changes required to prevent future data breaches
- Assess additional investment that may be required to implement recommendations
- Likely barriers to implementing improvements and how to overcome these

Evidence

- Identify and retain copies of all policies and procedures in force at the time of the incident.
- Identify all relevant training and retain copies of the materials and those who received it.
- Retain copies of all relevant system logs.

Distribution

- PO should receive the investigation report and recommendations.
- Share any lessons learned with relevant staff groups to reduce the likelihood of recurrence.
- Review lessons with third party providers and audit their systems.
- Outcomes should be recorded in writing and cross-referred to the University Risk Register.
- Significant failings should be referred to Audit and Risk Committee for consideration within the programme.

Personal data breaches are to be reported annually to Audit and Risk Committee, by the University Data Protection Officer, as part of the annual assessment of the University's response to data protection legislation. As introduced, above, significant instances of data loss may be reported to PO and/or Court outwith the annual reporting cycle.

Finally, StACSIRT should establish when the data breach is over, and the University response can be stood down.

6. Section 7 – Record-keeping and Debrief

Retention of records and documentation

Regardless of whether a personal data breach is to be notified to the relevant supervisory authority, a Controller [the University] is required to document all incidents of personal data breaches, however minor, and record [9] the:

- Facts relating to the breach;
- Effects of the breach (if any); and
- Remedial actions to be taken.

Records will also include the personal data breach classification assessment, and how that assessment was reached.

The University Information Governance and Assurance function maintains a personal data breach log and supporting information. This information will be held for a period of six years, after the last actions relevant to the breach have been concluded e.g. ICO investigation then destroyed.

Debrief on effectiveness of our response

A debrief review of the effectiveness of our response should be led by the IT Security Officer or Head of Information Assurance and Governance. For incidents categorised as Critical or Major, the debrief should be led by VP Gov or Quaestor.

The debrief should involve the entire core IMT, with non-core IMT involvement as required, and a written minute of the debrief and any associated recommendations should be stored with other evidence pertaining to the incident.

[9] GDPR, Article 33, paragraph 5.

7. APPENDIX A – Determining whether a Breach involves Personal Data

Purpose

Establish a controlled environment which, works to promptly to reach an informed understanding as to whether a data breach involves personal data or otherwise, from which point a breach can then be managed under the appropriate University plan.

What is a personal data breach?

A personal data breach, as defined by data protection legislation "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."[10]

For the purposes of this plan, a personal data breach will have occurred where:

- Data that falls within the legislative definition of personal data and that which falls within the definition of confidential or strictly confidential as defined by the University Information Classification Policy[11] is exposed to any entity or individual who is not authorised by the University, or through law to have access to those data. That may arise through:
    - a breach of physical or technical security leading to the accidental loss or theft of a device(s) or equipment, which holds information/data for which the University is responsible for the protection of; or
    - the accidental transmission of data to a person/entity e.g. sending a case file to the wrong solicitor etc.

And

- Where the security of ICT facilities/infrastructure provided by or through the University has become compromised or is suspected of having become compromised and there is a reasonable suspicion that personal data may be exposed to unauthorised persons.

Identification of a suspected or actual data breach or personal data breach

A data breach or a personal data breach could be identified through a range of University functions and associated processes, including:

- StACSIRT monitoring of the University network and associated services;
- Direct reporting or enquiry made to the IT Service Desk, IT Services;
- Direct reporting to the University's CSIRT and/or Information Assurance and Governance functions;
- Report of the theft of a device to the University Security function; and
- Report of the theft/loss/damage to a device, via an insurance claim or associated enquiry to the University Risk, Resilience and Insurance function.

[10] GDPR, Article 4, paragraph 12.
[11] Available, online: https://www.st-andrews.ac.uk/itsupport/itsecurity/classification/

What is a personal data breach?

A personal data breach will have occurred where personal data has become compromised, as per the criteria set out, above. See Does the data breach involve personal data, below for a definition of personal data.

Does the data breach involve personal data?

Are the data personal data, as defined by UK and/or European data protection legislation?
Personal data means data that falls within the following definition:

"'personal data' 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."[12]

[12] GDPR, Article 4, paragraph 1.

8. Appendix B - Personal data breach classifications

When assessing the classification of the personal data breach, the following categories are to be used:

- High i.e. there is a high risk to the rights and freedoms of individuals;
- Medium i.e. there is some risk to the rights and freedoms of individuals; and
- Very low i.e. it is unlikely that the breach will result in any risk to the rights and freedoms of individuals affected by the breach.

What categories of personal data breach require that notification to the ICO must be made?

The ICO only requires to be notified of a personal data breach where it [the breach] -
"…is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage."[13]

All personal data breaches classified as High and Medium must be reported to the ICO. A data controller is not required to notify where it has been assessed that a breach is unlikely to result in any risk to the rights and freedoms of individuals who have been affected by the breach.[14]

The Data Protection Officer is to be involved in decisions concerning the classification of a personal data breach and breach notification[15].

Risk assessment

In the absence of guidance from the ICO, risk assessment (whether a personal data breach is classified as high, medium or very low) is to be based upon the criteria set out in GDPR, Recitals 75 and 76 i.e.

Harm may arise from, exposed personal data being used in a way that would bring about:
physical, material or non-material damage, in particular: discrimination, identity theft or fraud, financial loss, damage to an individual's reputation, loss of confidentiality of personal data, or any other significant economic or social disadvantage;

individuals being deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures;

[13] ICO, Breach notification, available from: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/breach-notification/, accessed 13 September 2017.
[14] GDPR, Recital 85.
[15] GDPR, Article 39, paragraph 1(d).

An identification of an individual's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements; or where

A large amount of personal data is involved and this affects a large number of individuals.

The level of risk should be determined by assessing, on a case by case basis the scope, context and nature of the associated processing.

Provide context of harm, from ICO guidance as applied to breach 03-2018.

APPENDIX C – Personal Data Breach notification form (template)

This form is to be used when data controllers wish to report a breach of the Data Protection Act to the ICO. It should not take more than 15 minutes to complete.

If you are unsure whether it is appropriate to report an incident, you should read the following guidance before completing the form: "Notification of Data Security Breaches to the Information Commissioner's Office".

Please provide as much information as possible and ensure that all mandatory [*] fields are completed. If you don't know the answer, or you are waiting on completion of an internal investigation, please tell us. In addition to completing the form below, we welcome other relevant supporting information, eg incident reports.

In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

1. **Organisation details**
   a) [*] What is the name of your organisation – is it the data controller in respect of this breach?
   b) Please provide the data controller's registration number. Search the online Data Protection Public Register.
   c) [*] Who should we contact if we require further details concerning the incident? (Name and job title, email address, contact telephone number and postal address)

2. **Details of the data protection breach**
   a) [*] Please describe the incident in as much detail as possible.
   b) [*] When did the incident happen?
   c) [*] How did the incident happen?
   d) If there has been a delay in reporting the incident to the ICO please explain reasons for this.
   e) What measures did the organisation have in place to prevent an incident of this nature occurring?
   f) Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

3. **Personal data placed at risk**
   a) [*] What personal data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent.
   b) [*] How many individuals have been affected?
   c) [*] Are the affected individuals aware that the incident has occurred?
   d) [*] What are the potential consequences and adverse effects on those individuals?
   e) Have any affected individuals complained to the organisation about the incident?

4. Containment and recovery

a) [*] Has the organisation taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.

b) [*] Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

c) What steps has your organisation taken to prevent a recurrence of this incident?

5. Training and guidance

a) As the data controller, does the organisation provide its staff with training on the requirements of the Data Protection Act? If so, please provide any extracts relevant to this incident here.

b) Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?

c) As the data controller, does the organisation provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

6. Previous contact with the ICO

a) [*] Have you reported any previous incidents to the ICO in the last two years?

b) If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported and, where known, the ICO reference number.

7. Miscellaneous

a) Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.

b) Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.

c) Have you informed any other regulatory bodies about this incident? If so, please provide details.

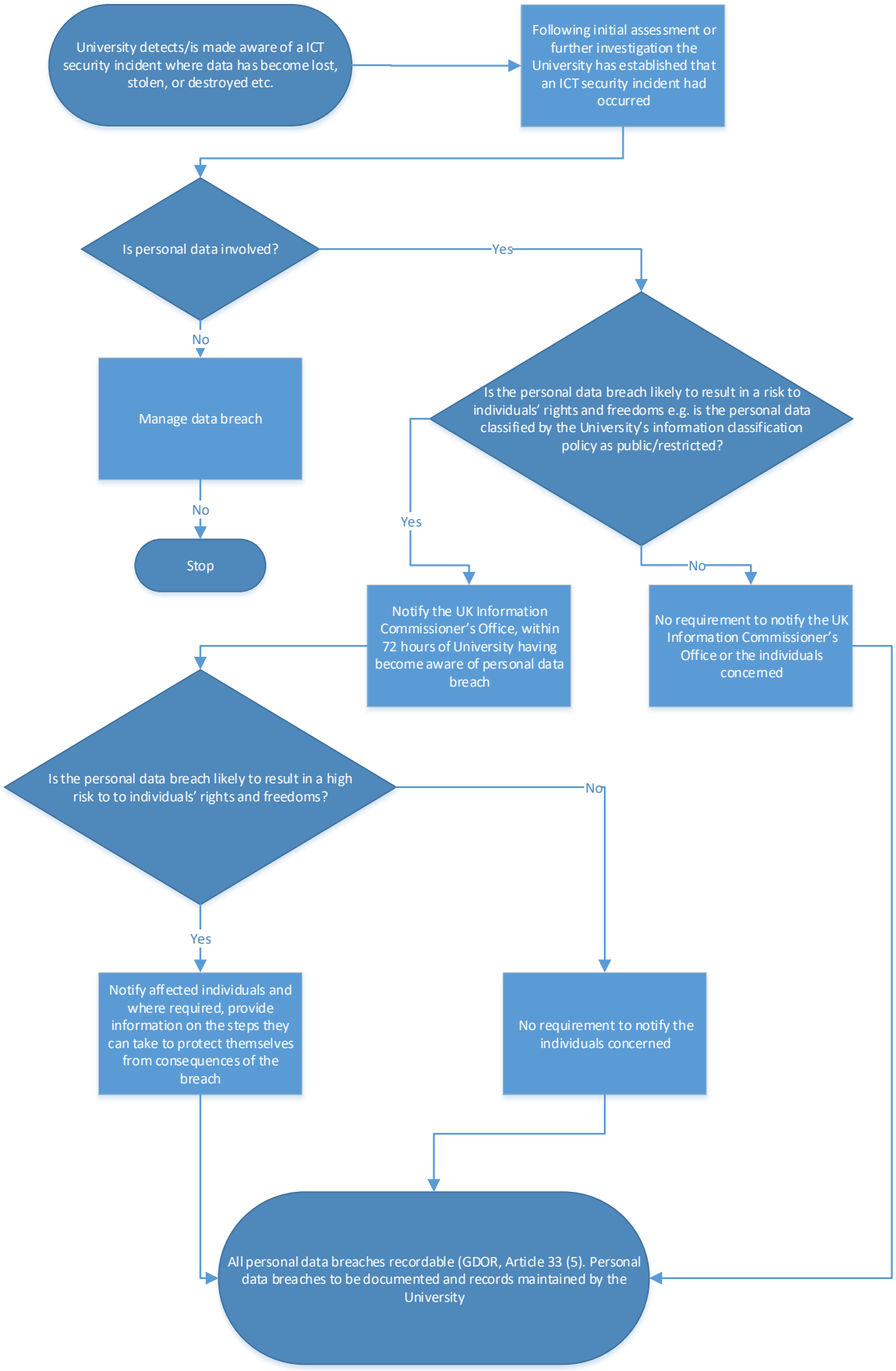
d) Has there been any media coverage of the incident? If so, please provide details of this.

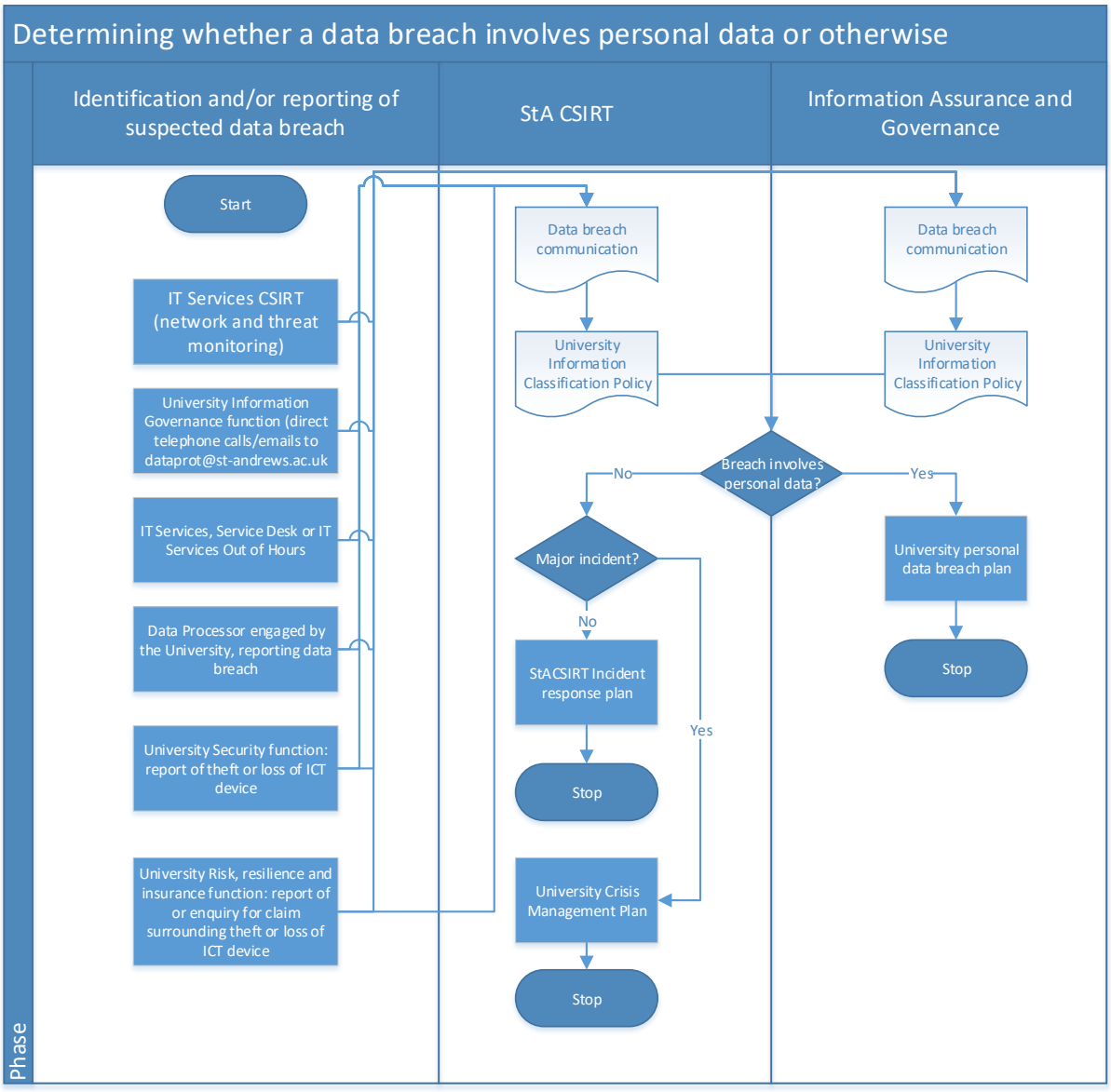
Sending this form

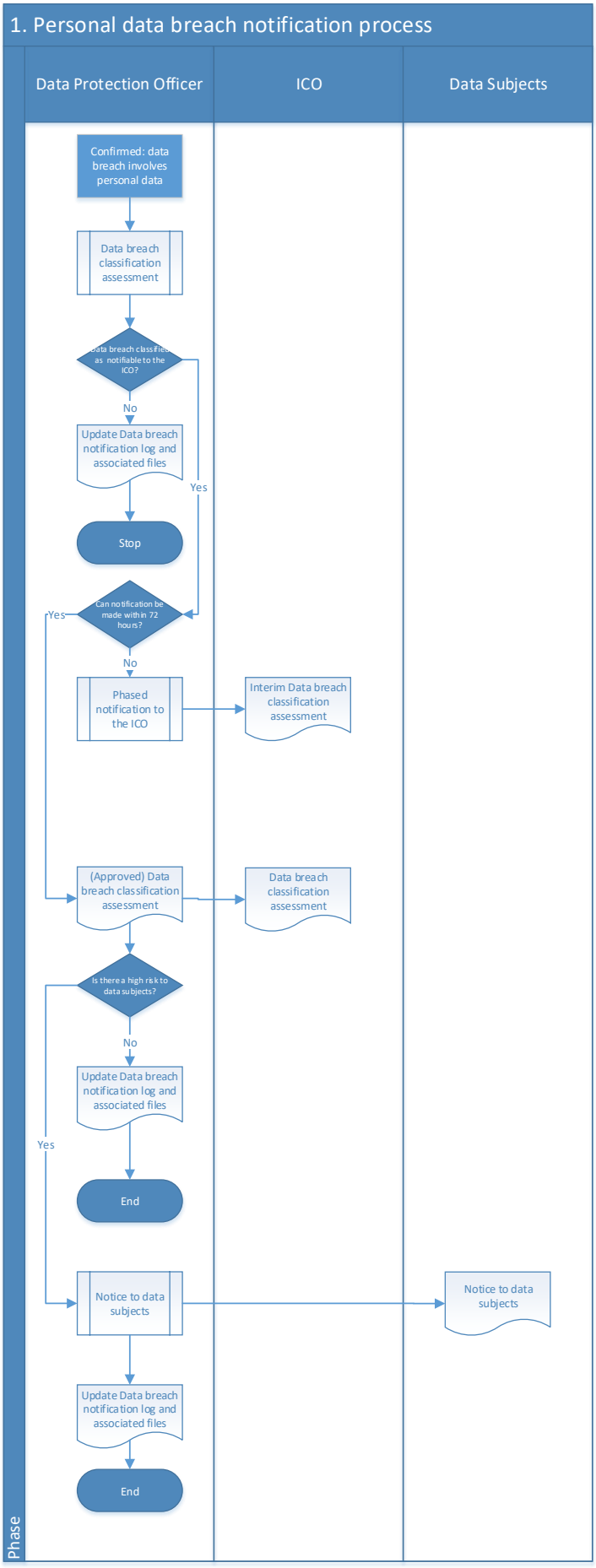
Send your completed form to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Please note that we cannot guarantee security of forms or any attachments sent by email.

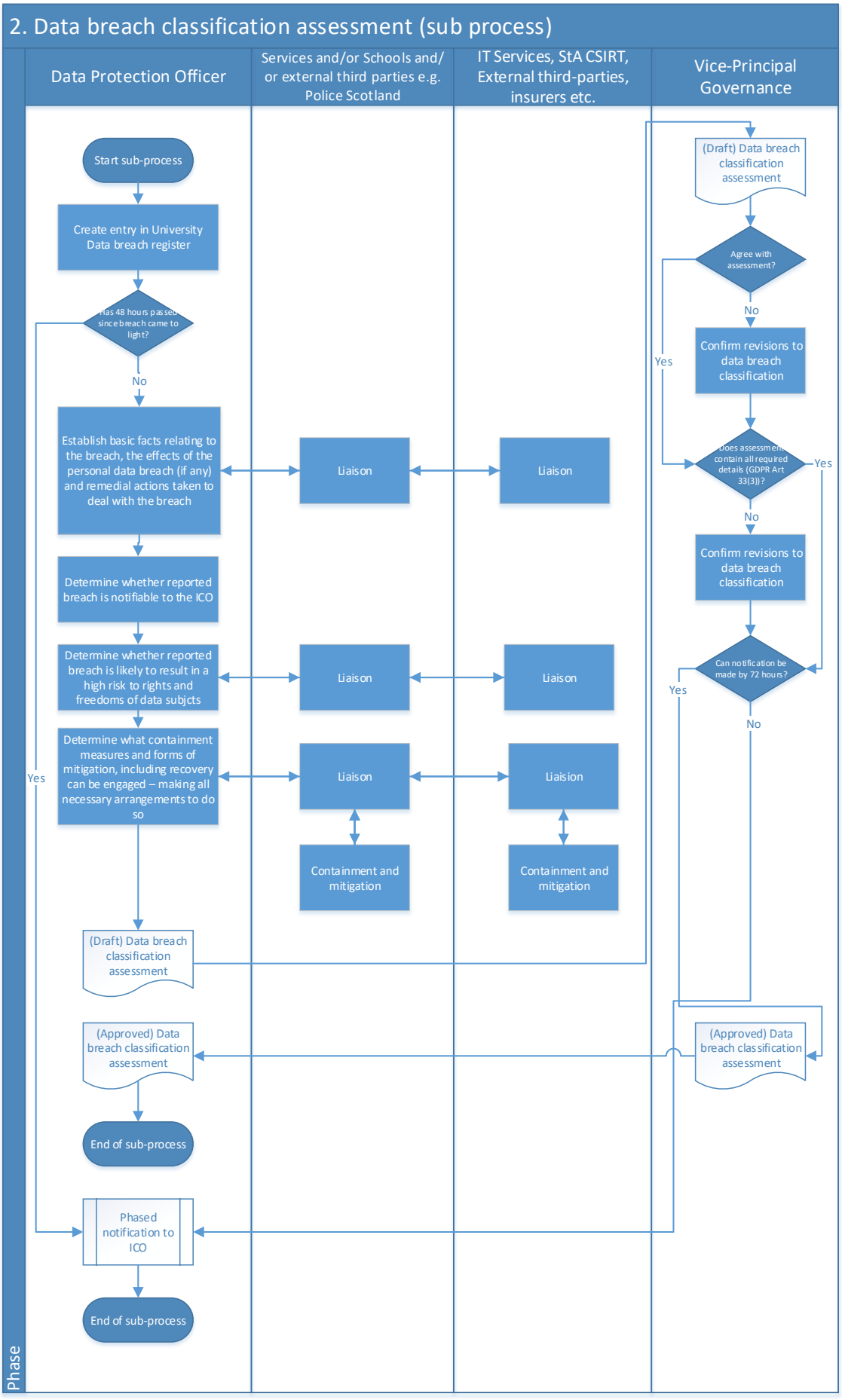
APPENDIX D - Information and Assurance GDPR Checklists

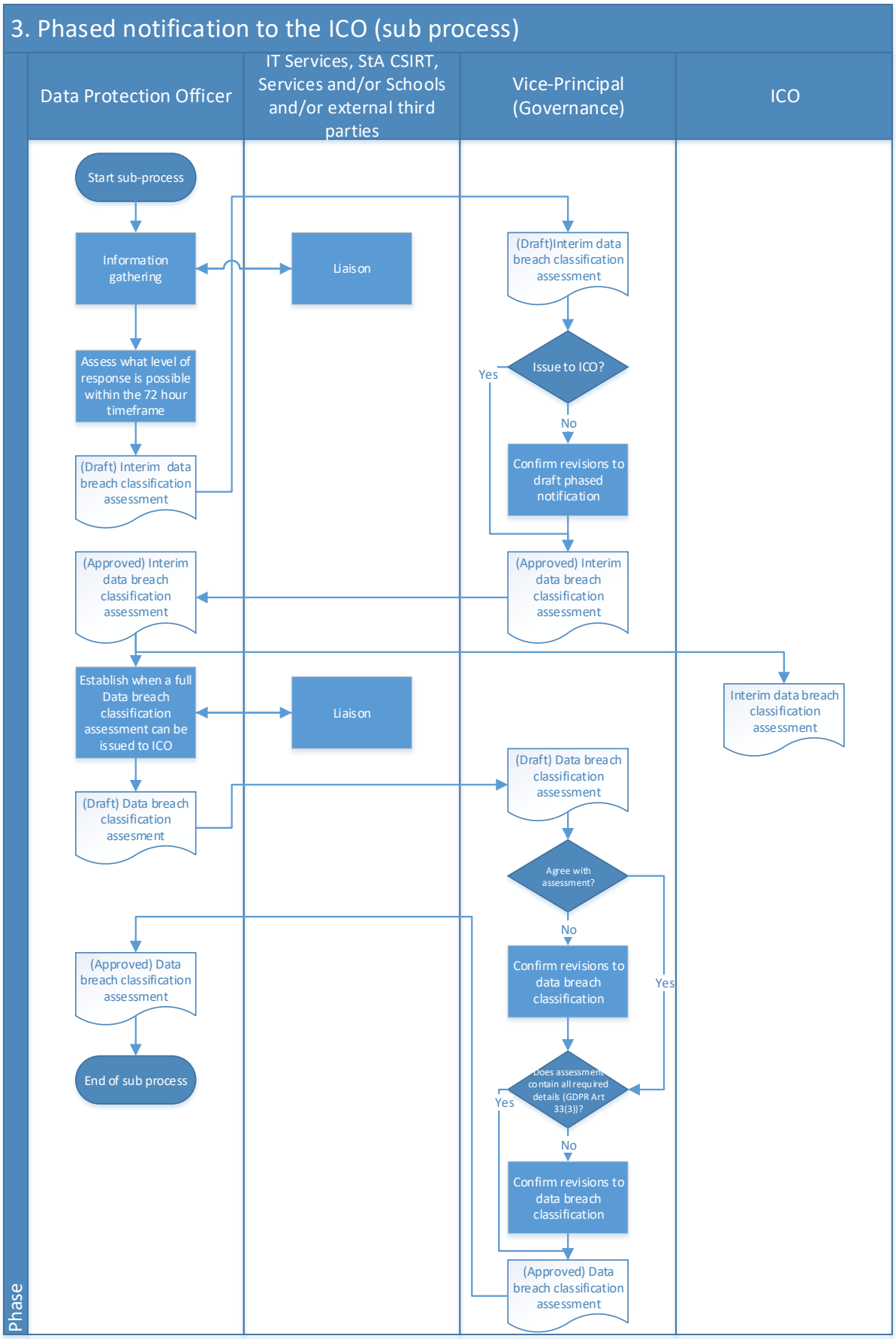
Overview

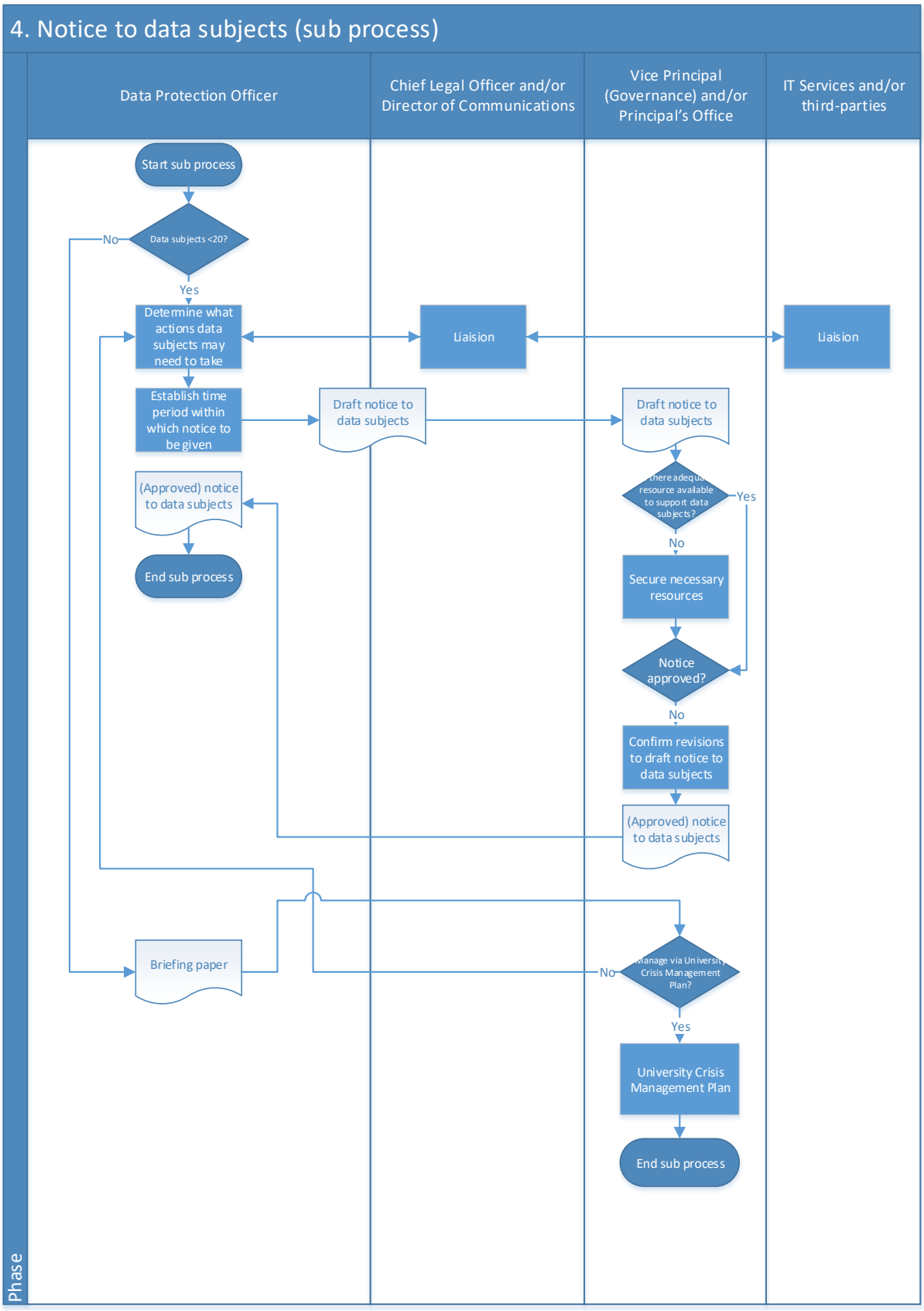



Determining whether a data breach involves personal data or otherwise
Identification and/or reporting of suspected data breach
StA CSIRT
Information Assurance and Governance
Phase
Start
IT Services CSIRT (network and threat monitoring)
University Information Governance function (direct telephone calls/emails to dataprot@st-andrews.ac.uk
IT Services, Service Desk or IT Services Out of Hours
Data Processor engaged by the University, reporting data breach
University Security function: report of theft or loss of ICT device
University Risk, resilience and insurance function: report of or enquiry for claim surrounding theft or loss of ICT device
Data breach communication
University Information Classification Policy
Data breach communication
University Information Classification Policy
Breach involves personal data?
No
Yes
Major incident?
No
Yes
StACSIRT Incident response plan
Stop
University Crisis Management Plan
Stop
University personal data breach plan
Stop


1. Personal data breach notification process
Data Protection Officer
ICO
Data Subjects
Confirmed: data breach involves personal data
Data breach classification assessment
Data breach classified as notifiable to the ICO?
No
Update Data breach notification log and associated files
Yes
Stop
Can notification be made within 72 hours?
Yes
No
Phased notification to the ICO
Interim Data breach classification assessment
(Approved) Data breach classification assessment
Data breach classification assessment
Is there a high risk to data subjects?
No
Update Data breach notification log and associated files
Yes
End
Notice to data subjects
Notice to data subjects
Update Data breach notification log and associated files
End
Phase


2. Data breach classification assessment (sub process)
Data Protection Officer
Services and/or Schools and/ or external third parties e.g. Police Scotland
IT Services, StA CSIRT, External third-parties, insurers etc.
Vice-Principal Governance
Start sub-process
Create entry in University Data breach register
Has 48 hours passed since breach came to light?
No
Yes
Establish basic facts relating to the breach, the effects of the personal data breach (if any) and remedial actions taken to deal with the breach
Liaison
Liaison
Determine whether reported breach is notifiable to the ICO
Determine whether reported breach is likely to result in a high risk to rights and freedoms of data subjcts
Liaison
Liaison
Determine what containment measures and forms of mitigation, including recovery can be engaged – making all necessary arrangements to do so
Liaison
Liaision
Containment and mitigation
Containment and mitigation
(Draft) Data breach classification assessment
(Draft) Data breach classification assessment
Agree with assessment?
No
Yes
Confirm revisions to data breach classification
Does assessment contain all required details (GDPR Art 33(3))?
Yes
No
Confirm revisions to data breach classification
Can notification be made by 72 hours?
Yes
No
(Approved) Data breach classification assessment
(Approved) Data breach classification assessment
End of sub-process
Phased notification to ICO
End of sub-process
Phase


3. Phased notification to the ICO (sub process)
Data Protection Officer
IT Services, StA CSIRT, Services and/or Schools and/or external third parties
Vice-Principal (Governance)
ICO
Start sub-process
Information gathering
Liaison
(Draft)Interim data breach classification assessment
Assess what level of response is possible within the 72 hour timeframe
Issue to ICO?
Yes
No
(Draft) Interim data breach classification assessment
Confirm revisions to draft phased notification
(Approved) Interim data breach classification assessment
(Approved) Interim data breach classification assessment
Establish when a full Data breach classification assessment can be issued to ICO
Liaison
Interim data breach classification assessment
(Draft) Data breach classification assesment
(Draft) Data breach classification assessment
Agree with assessment?
No
Yes
(Approved) Data breach classification assessment
Confirm revisions to data breach classification
End of sub process
Does assessment contain all required details (GDPR Art 33(3))?
Yes
No
Confirm revisions to data breach classification
(Approved) Data breach classification assessment
Phase


4. Notice to data subjects (sub process)
Data Protection Officer
Chief Legal Officer and/or Director of Communications
Vice Principal (Governance) and/or Principal's Office
IT Services and/or third-parties
Start sub process
Data subjects <20?
No
Yes
Determine what actions data subjects may need to take
Liaision
Liaision
Establish time period within which notice to be given
Draft notice to data subjects
Draft notice to data subjects
there adequate resource available to support data subjects?
Yes
No
(Approved) notice to data subjects
End sub process
Secure necessary resources
Notice approved?
No
Confirm revisions to draft notice to data subjects
(Approved) notice to data subjects
Briefing paper
Manage via University Crisis Management Plan?
No
Yes
University Crisis Management Plan
End sub process
Phase

APPENDIX E - Scottish Public Sector Incident Notification Template

Scottish Public Sector Cyber Incident Notifiable Report

(Revised May 2019)

Notifiable Scottish Public Sector Cyber Incidents are defined as incidents or attacks against Scottish public sector network information systems which:

- *have the potential to disrupt the continued operation of the organisation or delivery of public services; and/or*
- *carry a likelihood that other public, private or third sector organisations may experience a similar attack, or that the incident could spread to those organisations; and/or*
- *could have a negative impact on the reputation of the Scottish public sector or Scottish Government; and/or*
- *carry the likelihood of Scottish Parliament or national media interest.*

Scottish public sector organisations who are impacted by notifiable cyber incidents should **complete the notifiable cyber incident reporting form** below as early as possible and, if email services are available, send the completed form simultaneously to the following addresses in addition to those relevant to your own organisational requirements:

- The National Cyber Security Centre (NCSC):
- Incidents@ncsc.gov.uk
- The Scottish Government Cyber Resilience Unit (CRU): cyberresilience@gov.scot
- Police Scotland: C3DivisionServiceOverview@scotland.pnn.police.uk
- SGOR: SGORRInformation@gov.scot

These services are available 24 hours a day, 7 days a week, and can be contacted at any time in the event of a notifiable cyber incident. The 'follow up' numbers are as follows:

- **The National Cyber Security Centre (NCSC)**: 03000 200 973
- **The Scottish Government Cyber Resilience Unit (CRU)**: **0300 244 4000, ask for CRU Duty Officer**
- **Police Scotland :** 101 and ask for the Cyber Crime Unit On Call Officer
- **SGOR**: **07623 514719** (pager) SGOR Duty Officer

Where public sector organisations are aware that **sector / network-specific co-ordinating bodies** also have an interest, or role to play, in a notifiable cyber incident, they should copy these bodies into the email.

In the event that any **central co-ordinating body** (SG CRU, Police Scotland, NCSC) is notified of a notifiable cyber-incident involving a Scottish public sector organisation that has **not** been reported through the "Report it Once and Follow Up" procedure outlined above, it will seek agreement from the organisation affected to inform the other central coordinating bodies and sector/network-specific coordinating bodies.

PLEASE DO NOT FILL THIS FORM IN ON ANY NETWORK YOU BELIEVE HAS BEEN COMPROMISED. USE A SEPARATE SYSTEM TO FILL THIS IN.

Your Name

Your Phone

Your Contact Email Address

(The email address from an **uncompromised** system that all further correspondence should be sent to.)

Your Company Email Address

(The company email address for reference purposes (this may be compromised, but will not be used for correspondence)

What Organisation are you reporting an incident for?

What is your Role?

Summary of Incident

Are you sharing this with us for information or do you require advice and assistance from Police Scotland (investigation) NCSC (Incident Management) or SG CRU (Ministerial awareness or threat sharing)

- Select -

If assistance please specify

Do you have an Internal ID for the incident?

Investigation so far

Impact

- Select -

Description of Impact

Current state of incident

- Select -

Notification:

Have you reported this to:

Scottish Government Cyber Resilience Unit? ☐ Yes ☐ No

NCSC? ☐ Yes ☐ No

Police Scotland? ☐ Yes ☐ No

Information Commissioner's Office (ICO) as a GDPR obligation? ☐ Yes ☐ No ☐ N/A

Relevant Competent Authority (CA) as a NIS Directive obligation? ☐ Yes ☐ No ☐ N/A

Who else has been notified?

e.g external specialist response providers, Resilience Partners

Do you have any further data or samples to aid this incident? ☐ Yes ☐ No

Information Sharing:

Has any information been shared on the Cisp? ☐ Yes ☐ No

Do you have information you wish to have shared across the CREW network ? ☐ Yes ☐ No

If yes please provide the message content providing information that would enable other network defenders to take mitigating action.

Are there Media lines prepared is so can they be provided blow?

APPENDIX F – Template report

University of St Andrews
Incident report: [title]
[date]

[Template reporting form]

[V1.0 January 2019]

[This version not to be used for HR investigations]

[Incident classification – from spreadsheet]

9. Overview

[Summary of what happened]

10. Incident details

[Key events]

[Analysis]

11. External reporting

[Note any external reporting that might need to be done]

12. Containment and Recovery

[What has been done to contain and recover from the incident]

13. Risk

[On going risk factors]

[Secondary / residual risk]

14. Timeline

Dates	Activity	Comment

15. Limitations

[Note any limitations to the investigation]

16. Next Steps

[Lessons learnt]

[Next steps, by whom]

Version number	Purpose / changes	Document status	Author of changes, role and school / unit	Date
1.0	Procedure incorporates previously approved procedures for data and personal data breaches	Approved		