ACRO Data Breach Guidance

And Standard Operating Procedure

ACRO Criminal Records Office
enquiries@acro.pnn.police.uk | acro.police.uk | @ACRO_Police

Product Control Page

Version No.	Date	Amendments Made	Authorisation
0.1		Initial draft	[redacted]
0.2	09/05/2016	Minor Update	[redacted]
0.3	09/06/2016	Minor Updates	[redacted]
0.4	20/06/2016	Updates following consultation	[redacted]
0.5	28/06/2016	Change to indemnity	[redacted]
1.0	06/07/2016	Finalised	[redacted]
1.1	19/01/2018	Updates; new regime referenced	[redacted]
1.2	19/02/2018	Updates; SMT recommendations	[redacted]
1.3	07/03/2018	Restructured and detail added	[redacted]
1.4	10/04/2018	Updates; SMT recommendations	[redacted]
2.0	17/04/2018	Signed off by ACRO Information & Technology Board	[redacted]
2.1	05/03/2019	Revision of process as agreed by AITB February 2019 and update on ICO penalties	[redacted]
2.2	14/08/2019	Updated procedure and HR amendments	[redacted]
2.3	22/08/2019	Data breach logger	[redacted]
2.4	11/11/2019	HR Updates	[redacted]
2.5	03/12/2019	Reviewed numbering and added Probation policy	[redacted]
2.6	09/03/2020	Steering/working groups added Policy changed to Guidance	[redacted]
2.7	19/03/2020	Home working added	[redacted]

2.8	19/07/2021	Updated wording under legal requirements (DPA 2018)	[redacted]

Index

1. Guidance

1.1 ACRO Criminal Records Office complies with the host force Data Protection Policy and subsequent Policies and Procedures, these are referenced at *Appendix 1*.

1.2 The Data Protection Act 2018 places certain obligations on organisations and staff when dealing with personal data, including the obligation to provide personal data with the appropriate technical and organisational protection measures against unauthorised or unlawful processing and against accidental loss or destruction of, or damage to, personal data.

1.3 ACRO is committed to meeting its obligations as a Data Processor to the police service, as agreed under s22A of the Police Act 1996. In the event of a data breach we will assess whether the Data Controller needs to be notified.

1.4 ACRO is committed to proactive fulfilment of its security obligations when processing personal data and taking prompt, appropriate action when a breach occurs to protect the data subject(s) and their data.

1.5 The purpose of this document is to provide details of managing and handling a suspected or actual data breach in order to protect both the data subject(s) and the organisation. It is intended to improve data breach handling from past lessons learned[1], while meeting legislative requirements.

1.6 ACRO is a progressive organisation committed to processing personal data securely and learning lessons from breaches, taking appropriate action to avoid the same or similar breaches from reoccurring.

1.7 To demonstrate this commitment to learning, ACRO mandates that all staff attend in-house data breach awareness training to mitigate the risks associated with data breaches and to ensure the proper response when a data breach is suspected or detected.

1.8 Where appropriate, ACRO will self-refer data breaches to the Information Commissioner's Office (ICO).

1.9 When a breach is reported to the ICO, there is the possibility of the ICO levying a Civil Monetary Penalty for failure of processing obligations. This could be up to 10 million euro or 2% of annual turnover. Failure to comply with core principles, data subject rights, statutory obligations, orders to cease processing or grant access to ICO or failure to comply with provisions on overseas transfers, could result in penalties of 20 million euro or 4% annual global turnover, whichever is higher. Should the organisation self-report to the ICO, prompt action and taking corporate ownership of the breach investigation demonstrates good practice.

1.10 Self-reporting to the ICO should not be seen as a negative step, as proactive self-reporting can reduce or negate any Civil Monetary Penalty levied. Prompt, appropriate action can result in the ICO choosing not to levy a Civil Monetary Penalty, opting for a lesser determination such as an undertaking, or enforcement notice.

1.11 ACRO has secured insurance under the Professional Indemnity policy whereby ACRO pays the first £250,000 as an excess for any settlement where the data subject seeks damages through the Courts.

[1] Data Breaches – Lessons Learned: Update for the ACRO Information & Technology Board, 20TH September 2017, ACRO National Services

2. Roles and responsibilities

2.1. Staff Member

2.1.1 Immediately alert Head of Section (HOS)/Supervisor that a data breach or near miss has occurred, both verbally and by completing the Data Breach Logger located on the ACRO Intranet on the Data Protection tile. The Data Breach Logger will allocate a unique reference number to the breach, automatically populate the data breach log, initial report and email to be sent to the Supervisor by the breach identifier. If their HOS/Supervisor is not available the staff member will need to inform a HOS/Supervisor from their area or from another portfolio to ensure the breach is risk rated within the 72 hour requirement made by the Data Protection Act 2018. In addition to sending the email ensure the HOS/Supervisor is verbally informed to expect the email.

2.2. Duty Officer (Business)

2.2.1 If the Duty Officer receives a report of a breach out of hours, they will follow the instructions for a Staff Member and complete the initial incident report. The Duty Officer will complete the Data Breach Logger Part One, Review and Deputy Managers' sections, to complete the risk rating section. They will complete the matrix to assess whether it is necessary to contact the Data Protection Officer or Head of ACRO out of hours. The escalation point being an identified risk rated Amber or Red where immediate action needs to be taken and/or an ICO referral will need to be considered.

2.3. Head of Section/Supervisor

2.3.1 Upon receiving the email with the link to the Data Breach Logger and reference number, the HOS/Supervisor will review the information entered into the Data Breach Logger updating and amending where necessary. They will need to allocate a Deputy Manager to escalate the breach to for risk rating. The Logger will automatically update the data breach log, initial report and create the email to escalate the breach to a Deputy Manager. If their Deputy Manager is not available the HOS/Supervisor will need to inform a Deputy Manager from another portfolio to ensure the breach is risk rated within the 72 hour requirement, made by the Data Protection Act 2018. If the breach is related to IT the IT Senior Manager should also be notified. Immediately carry out any remedial action as required. Ensure out of hours breaches are escalated as appropriate by contacting the Duty Officer (Business), Data Protection Officer or Head of ACRO.

2.3.2 HOS/Supervisor is responsible for monitoring the data breaches for their members of staff and taking action, as appropriate, in accordance with the managing performance policy.

2.4. Deputy Manager

2.4.1 The Deputy Manager will complete Part Two Review and Risk rating, of the Data Breach Logger. Using the notification matrix, (Appendix 2 Notification Matrix – Guidance and Appendix 3 Notification Matrix – Impact Assessment), complete an assessment of the risk to the data subject/s. In line with the risk rating, escalate if necessary and issue instructions regarding any remedial action or investigation. If the risk is rated green the Logger will update the data breach log, incident report and the breach will be closed. If the risk rating is deemed to be Amber or Red the Deputy Manager will inform a Senior Manager in person or by phone for guidance and advice. The Deputy Manager will escalate the breach via the Data Breach Logger's generated email, for the SMT to review.

2.4.2 Deputy Managers are responsible for monitoring data breaches in their business area and ensuring that a fair and consistent approach is taken in managing the data breaches and that any action taken is in accordance with the managing performance policy.

2.4.3 Where further actions are required the Deputy will be tasked by the SMT to carry out any investigation and ensure that actions are complete.

2.5. Senior Manager

2.5.1 The SMT will be informed of any breaches that are risk rated Amber or Red by the Deputy and will re-assess the risk rating using the matrix at appendix 2 and the impact assessment at appendix 3. The risk rating may be down-graded once the potential impact on the data subject is established after an initial investigation. Any high Amber or Red breaches MUST be reported to the ICO. This should be done via the Data Protection Officer (DPO) as the single point of contact for the ICO, after agreement by the Head of ACRO or CEO.

2.5.2 In the event that the DPO, Head of ACRO and CEO are not available the SMT will need to make a judgement call as it is imperative that the breach be reported to the ICO within 72 hours of being identified.

2.5.3 The SMT will receive an email linking to the Data Breach Logger, they will review the form and complete part three. If an ICO referral is required they will access the initial incident report by using the case file link on the Data Protection intranet page. These are stored under the relevant breach number. The report should be sanitised of any third party data and any explanations made clear. The ICO copy should be given an appropriate title. This will be sent to the DPO, or in their absence directly to the ICO at the address icocasework@ico.org.uk.

2.5.4 The Senior Manager for IT should also be informed of any IT related breaches.

2.5.5 Please note that the Information Manager will provide assistance in the absence of the DPO.

2.5.6 When access to the data breach logger is prevented due to home working or IT issues the SMT can use their discretion to adapt local processes to ensure that the breach is logged properly and within 72 hours.

2.6. Data Protection Officer (DPO)

2.6.1 The role of the DPO is to advise staff how to risk assess and manage data breaches, and to act as the conduit between ACRO and the ICO office. The DPO will attend Gold Groups in an advisory capacity.

2.7. Information Manager (IM)

2.7.1 To ensure that the Data Breach Logger is completed appropriately. The IM Will be responsible for ensuring all data breaches are properly managed, reported and any remedial actions are taken. To look at lessons learned and ensure that changes are implemented where appropriate. To report all breaches and near misses to the appropriate boards. To review the ACRO Data Breach Guidance on a regular basis.

2.8. Head of ACRO & Chief Executive Officer

2.8.1 To receive, review and sign off on any self-referrals to the ICO and to Chair the Gold Group. To ensure that data breaches are reported to the relevant boards and own the guidance for managing data breaches. Head of ACRO to provide advice and guidance to Deputy Manager/Duty Officer for breaches, occurring out of hours, risk assessed as Amber or Red.

2.9. Gold Group

2.9.1 The Gold Group will consist of the following members;

- Chief Executive Officer
- Head of ACRO
- Data Protection Officer
- Information Manager
- Senior Manager dealing
- Deputy for the relevant Portfolio
- IT Manager when required
- Other members as required on a case by case basis

2.9.2 The Head of ACRO or CEO will decide if a Gold Group is required, or in their absence the SMT dealing. Members will be informed of the breach by email and will attend a meeting if requested. An update on the breach will be provided at the following ACRO Information and Technology Board (AITB) which will be attended by Gold Group members.

2.9.3 The Gold Group will be responsible for ensuring that all required action is taken in relation to the breach;

- Establish breach circumstances and enter in breach log
- Identify data involved
- Assess risk to the data subject(s)
- Retrieve data
- Consider informing the data subject(s) and engaging public protection measures
- Consider informing the data controller
- Consider self-referral to the Information Commissioner (ICO)
- Implement actions to prevent future breach
- Liaise with force insurance / solicitor
- Ensure correct recording of breach for subsequent analysis and organisational learning

2.10 Data Breach Process Map

2.10.1 The steps to report a data breach, near miss or dispute are outlined in the full data breach process map at *Appendix 4.*

2.10.2 Links to individual process maps by role are located at *Appendix 5*.

2.10.3 A quick one page flow diagram is available at *Appendix 6*.

2.10.4 A quick reference one page guide is available at *Appendix 7*.

3. Definitions

3.1 Data Breaches

3.1.1 Data breach refers to non-compliance with one or more of the data protection principles. The following list includes some common scenarios that can constitute a data breach:

- Inappropriate verbal disclosure of personal data
- Personal data sent by email to the wrong recipient
- Personal data posted or faxed to the wrong recipient
- Loss or theft of paperwork containing personal data
- Misplacing paperwork or mobile devices storing personal data
- Insecure disposal of paperwork containing personal data (not using confidential waste bins)
- Processing personal data relating to work on an insecure non-business computer or device
- Failure to redact personal data, particularly regarding third parties
- Hosting an insecure web-page which can lead to hacking and access to personal data
- Personal data inappropriately uploaded to a web page
- The loss or theft of an unencrypted device containing personal data
- Insecure disposal of hardware containing personal data
- Disclosure of inaccurate data
- Unauthorised access to personal data
- Unintended loss of access to personal data even if it is temporary and the data is not disclosed (Exceeding 4 hours or whenever there is a significant impact to the business whichever is soonest)
- Accidental or intended damage to personal data

3.1.2 Other non-compliance with the data protection principles can also constitute a breach, unless exempted or allowed by legislation.

- Unreasonable inaccuracy of personal data
- Unlawful or excessive processing of personal data
- Excessive retention of personal data
- Unauthorised, excessive access to personal data

3.1.3 Data breaches not only require immediate action to investigate and contain the situation, but also a recovery plan, including consideration of damage limitation both for the data subjects involved, the data controller and the organisation. This may even include implementing public protection measures to protect the data subject(s) where significant risk to them is identified.

3.2 Near Misses

3.2.1 A near miss is where part of the process would have resulted in a data breach, but an individual has identified it before the breach has taken place. The recording of near misses is required throughout all ACRO business areas.

3.2.2 For example, a near miss could be a member of staff addressing an envelope incorrectly, another staff member identifies the error prior to it being posted, thus preventing a data breach.

3.2.3 These near misses are reported via the Data Breach Logger to be reviewed by the Head of Section/Supervisor and referred to the Deputy Manager. There is no further escalation and the logger will close the near miss.

3.2.4 The purpose is for Deputy Managers and the Information Manager to review whether there is a training requirement, or change in process necessary to avoid possible breaches in the future.

3.2.5 Near misses, that would be risk rated amber or red if they had resulted in breaches, are reported to the Home Office on a quarterly basis for review. This report is submitted to the ACRO Information and Technology Board for information.

3.3 Lost in Post

3.3.1 'Lost in Post' (LiP) refers to Letters, Disclosures or Certificates that do not arrive at the requested destination and it is unknown where the data has arrived/is being held.

3.3.2 The Data Protection Act states that 'personal data should be processed in a manner that ensures appropriate security… including protection against…accidental loss'.

3.3.3 Any correspondence not delivered to the intended address, is a data breach and ACRO is held responsible, as they remain the data controller and data processor.

3.3.4 ACRO's preferred carriers are Royal Mail for postal deliveries and City Sprint for courier service. Responsibility for delivery still lies with ACRO who should ensure that any method of data transfer is secure throughout the process.

3.3.5 All items LiP must be recorded in the Customer Services 'Lost in Post' spreadsheet which will include statistical information of volumes. This will be reliably sourced from data extracted from the GSA database and updated on a weekly basis by the Customer Services Head of Section.

3.3.6 There is no requirement to report these to a Deputy Manager, Senior Manager or Data Protection Officer, or to complete the Data Breach Logger.

3.3.7 The Information Manager will be responsible for monitoring these breaches and ensure any remedial action is implemented to minimise losses. A report will be submitted to AITB on a monthly basis.

4. Standard operating procedure

4.1 Data Breach Log

4.1.1 The Data Breach Log is a master spreadsheet which is populated by information input into the Data Breach Logger. This is used by the Information Manager to monitor reported breaches ensuring all sections of the Breach Logger are fully completed. It is also used to gather the statistical data for reporting to the Portfolio, AITB, Home Office and Governance Boards.

4.2 Incident Report

4.2.1 The Incident Report is generated by the information input in the Data Breach Logger. The Logger automatically allocates a data breach reference number to each new breach entered.

4.2.2 This document will be redacted and sent to the ICO if a breach is significant and requires self-referral to the ICO.

4.2.3 The Incident Reports are also reviewed when compiling the quarterly report on data breaches for submission to the Home Office.

4.3 Data Breach Logger

4.3.1 The member of staff reporting the breach/near miss will access the data breach logger from the Data Protection page on the ACRO intranet.

4.3.2 In the event that the staff members finds a fault with the log this should be reported immediately to Information Management.

4.3.3 When access to the data breach logger is prevented due to home working or IT issues the SMT can use their discretion to adapt local processes to ensure that the breach is logged properly and within 72 hours.

4.4 Remedial Action

4.4.1 Immediate remedial action to contain the impact of a data breach must be taken to protect the data subject and their data, which has been disclosed, and mitigate possible adverse effects. HOS/Supervisors must take prompt, appropriate action when a breach occurs.

4.4.2 Advice is to be sought from Deputy Managers, Senior Managers, the Information Manager and Data Protection Officer to ensure that ACRO are compliant in managing the breach efficiently and effectively.

4.4.3 Damage limitation, both for the data subjects and the organisation, needs to be considered. This may include implementing public protection measures to protect the data subject(s) where significant risk to them is identified.

4.4.4 If it is identified that there is an immediate risk to a data subject the Senior Manager/Head of ACRO must ensure safety measures are implemented and call a Gold Group meeting to ensure that adequate steps have been taken.

4.5 Initial Report to ICO

4.5.1 In the event that an ICO referral is required, the Senior Manager will contact and discuss the incident with the Head of ACRO or Chief Executive Officer with the recommendation for self-referral. The initial report will be sent to the Information Manager and Data Protection Officer for review and advice.

4.5.2 A Gold Group should be formed for all referrals to the ICO, the Head of ACRO /Chief Executive Officer should decide whether a meeting is required.

4.5.3 Where self-referral to the ICO is authorised the Senior Manager should send a de-personalised copy of the completed initial incident report to the ICO.

4.5.4 Investigation of the actual or suspected breach should normally commence within 24 hours of detection, with the initial determination complete within 72 hours, unless exceptional circumstances are described.

4.5.5 A national guide on notifying the ICO can be found at *Appendix 8* and the outcome of notifying the ICO can be located at *Appendix 9*.

4.6 Next Steps

4.6.1 The Deputy Manager will ensure that the following steps are carried out.

4.6.2 Request that the recipient returns the documentation to ACRO in respect of a certificate, or alternatively that the recipient has deleted or securely disposed of the personal data they received in error.

4.6.3 You should then decide whether it is appropriate or necessary to inform the data subject of the breach.

4.6.4 Where ACRO is processing the data on behalf of another data controller or partner organisation, consideration should be given by the Deputy or Senior Manager about reporting the breach to the data controller or partner organisation as soon as possible in case they need to implement public protection measures.

4.6.5 The data subject and the data controller(s) will be notified of ALL cases resulting in a self-referral to the ICO.

4.6.6 Where a self-referral is made to the ICO, the Senior Manager for the relevant portfolio will be the SPOC while the investigation remains open.

4.6.7 Where a self-referral is made to the ICO the SPOC will be responsible for ensuring that the Gold Group is kept updated.

4.7 Final ICO Report

4.7.1 After the initial report has been sent to the ICO the Senior Manager will commission a further investigation and submit a final report via the DPO to the ICO within 28 days. A draft final report can be located from the ACRO Data Protection intranet page.

4.7.2 The SPOC will consult with the Data Protection Officer and Information Manager while completing the final report, submitting it to the Chief Executive Officer and Head of ACRO prior to sending it to the ICO.

4.7.3 The ICO will respond to the report with a decision and recommendations. The DPO will be responsible for updating the Gold Group, and the Information Manager will write a summary report for AITB. This will summarise the nature of the breach, the action taken, the ICO decision and recommendations, and whether these have been implemented.

4.7.4 A sample of the final report to the ICO can be located at *Appendix 10.*

4.8 Lessons Learned

4.8.1 An organisational lessons learned will be published with the assistance of the Communications Team quarterly. The information for the publication will be taken from the Data Breach Master spreadsheet.

4.8.2 The Deputy Manager will be responsible for identifying lessons learned for each breach they are managing and update the Logger accordingly.

4.8.3 In respect of ICO referrals, the SPOC will make the decision as to whether it is necessary to update the Gold Group on lessons learned, as part of the breach investigation or on communication received from the ICO.

4.8.4 The Information Manager will have oversight of the recording of all data breaches. They will ensure that all elements of the guidance are adhered to and, if necessary, will chase up outstanding tasks.

4.8.5 The Information Manager will look at the trends in the data breach log and will look at whether additional training has been provided or processes have been changed. They will liaise with the relevant Senior Manager and Deputy Managers to achieve this.

4.8.6 The Information Manager will review the lessons learned and will make recommendations to the AITB for any further changes required as a result of their findings.

4.9 Reporting

4.9.1 All staff are responsible for reporting data breaches and near misses as they are identified.

4.9.2 HOS/Supervisors are responsible for reviewing data breaches reported to them and escalating as necessary.

4.9.3 The Deputy Manager is responsible for ensuring that each breach is reported and managed appropriately.

4.9.4 Where a Gold Group is formed the Senior Manager is responsible for updating them throughout the process.

4.9.5 The Information Manager is responsible for reporting a summary of all data breaches to the AITB, Home Office and ACRO Governance Board, including updates on any self-referrals to the ICO. They are also responsible for reporting any lessons learned and recommendations.

4.9.6 The Information Manager will produce a monthly report for AITB. Quarterly reports will be submitted to the Home Office and ACRO Governance Boards, these will summarise the data breaches and any changes that were implemented as a result.

4.10 Performance Management

4.10.1 Unsatisfactory performance occurs where an individual is unable to perform the duties of their role to a satisfactory standard or level.

4.10.2 A significant data breach (or series/trend of data breaches) could be identified as a performance concern and result in an individual being subject to action under the managing performance policy.

4.10.3 In the event that an individual demonstrates wilful or negligent behaviour that results in a data breach, action may be considered under the managing misconduct policy – police staff.

4.10.4 Statistical data in support of individual data breaches will be provided to the ACRO SMT by the Information Manager. The ACRO SMT will be responsible for reviewing cases and agreeing the most appropriate action.

4.10.5 An HR guide on manageing performance is available at Appendix 11

4.11 Steering Group

4.11.1 The Steering group, Chaired by the DPO or Information Manager, will meet on a quarterly basis. Regular attendees will include the SMT for National Services, International Services and Projects & Intelligence. An HR Manager or advisor will attend to advise on HR policy. Other SMT may be invited if staff in their business areas require discussion.

4.11.2 A referral to the Steering Group can come from Information Management, or a Senior/Deputy Manager who may have concerns about an individual who has made a significant breach, or multiple breaches.

4.11.3 In advance of the meeting the Information Manager will provide attendees with performance data about any staff member to be discussed.

4.11.4 The Steering Group will consider all available information, including the following;

- The volume of work undertaken by the individual
- The training provided to the individual
- Whether the individual has been spoken to previously about breaches
- The hours and pattern worked and output
- What processes they are undertaking
- Any mitigating factors which may help to explain why a breach occurred.

4.11.5 Outcomes could include NFA, management advice, training or more formal action in line with the appropriate procedure. Decisions are to be made in collaboration with the HR team and recorded to ensure fairness and consistency.

4.11.6 Outcomes from the Data Breach Steering Group should be anonymised and high level data provided to ensure staff awareness of breaches. This will seek to inform organisational learning and help to prevent further breaches.

4.11.7 A Steering Group flow diagram is available at appendix 12.

4.12 Working Group

4.12.1 Changes may be required to the breach management process as a result of changes to information systems, national policy or procedure or ACRO processes.

4.12.2 Before carrying out any changes a working group will be formed to discuss the impact of any changes on each business area. The working group will be chaired by the Information Manager and attended by Deputy Managers representing and business areas that may be affected by the proposed changes.

4.12.3 Any proposed changes will be ratified by the ACRO Information and Technology Board (AITB) and will subsequently be updated in this guidance.

5. Appendices

Page Intentionally Blank

Appendix 1 – Related Policy & Procedure

Further information regarding the policy and procedure can be obtained on the Intranet.

- JIMU Information Security Policy 90000
- Security and Information Assurance Policy 06100
    - IT Security Management Policy 28400
    - ACRO Data Protection, published on the ACRO Intranet Pages
    - Data Protection Procedure – 02106
    - Access Procedure – 06103
    - Information Sharing Procedure – 30802
    - Information Security Guidance
- User Responsibilities in respect of information processes procedure 06101
- Force Homeworking Security Procedure 06102
- Protective Marking Procedure 06109
- Performance Management Policy
- Probationary period of Police Staff 33013

Appendix 2 - Notification Matrix - guidance

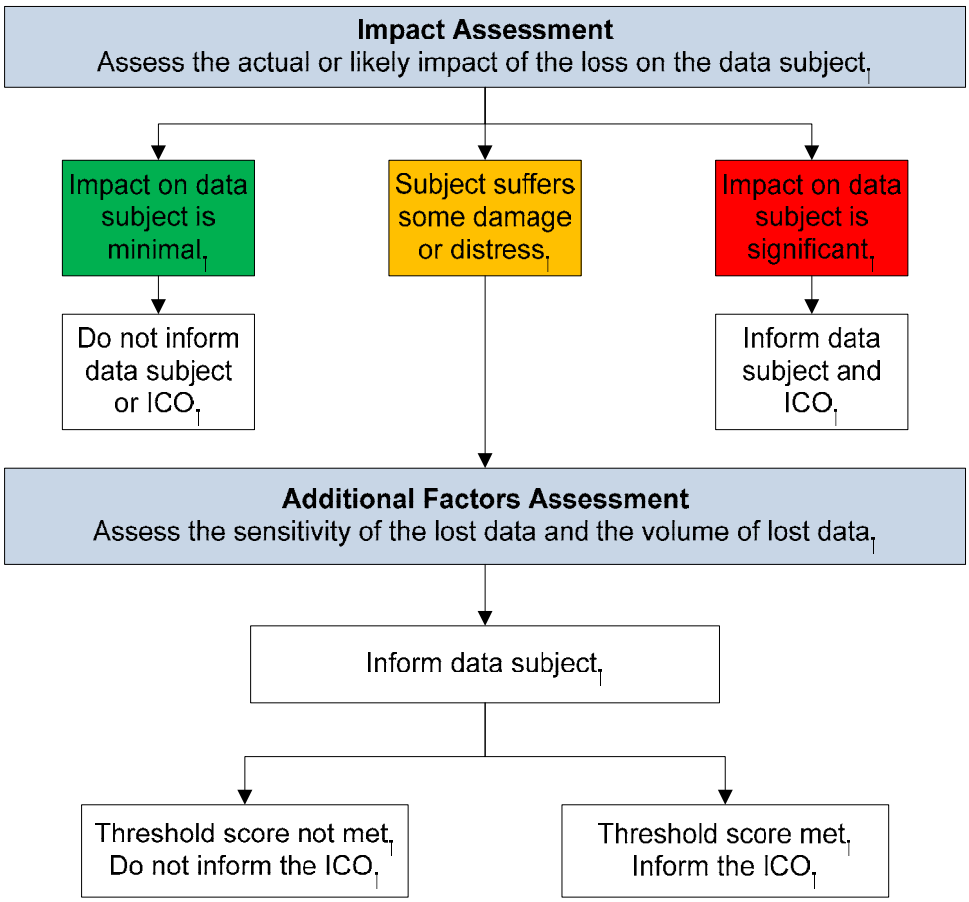
The notification matrix will be revised as of May 2018. Any breach indicating a risk to the rights and freedoms of the data subject will become notifiable.

The Notification Matrix on the following pages will help to determine whether a loss, theft, unauthorised disclosure or compromise of personal data is 'significant' and therefore should be reported to the ICO. Fundamental to this matrix is the use of the National Decision Model and that normal force policies such as Critical Incident investigation are not superseded by it, but that factors are considered in light of it.

The use of individual discretion is not prevented. Acting outside of this guidance is permitted where the decision can be justified and the rationale is recorded in sufficient detail. Examples of circumstances where the use of discretion may be considered are where the loss is a repeated incident or where there is significant impact on public confidence, which may lean in favour on notification. Adherence to the Code of Ethics may facilitate making discretionary decisions of the highest professional standards of public service.

Whilst the model below is purely referring to the data subject and ICO notification, it is expected to operate within, and therefore also be assessed within the operational context of any related / directly connected incident. This will ensure that the primary concern of public safety is always paramount.

The rationale and outcome of notification decisions should be recorded on the Data Breach Investigation Checklist.



When using the Notification Matrix to assess all three of the above assessment factors (impact, sensitivity and volume) it is not necessary to satisfy all the criteria in a particular box. A 'best fit' approach is advised. Regardless of the outcome, the decision and rationale behind it should be recorded.

Timing of any notification

If the outcome is to notify the ICO of the data protection breach, consideration must be given as to when to notify. Ordinarily notification should occur as soon as the information required in the ICO's Notification Form is available (further information about what is required is listed in Appendix A). However; consideration must be given as to whether notifying the ICO could prejudice an ongoing investigation or operation and if so it may need to be delayed.

The decision whether or not to self-refer to the ICO will be made by the NPCC Director of Information as well as the referral itself.

As of May 2018, if the notification is not made within 72 hours, exceptional circumstances must also be described to the ICO.

Appendix 3 – Notification Matrix - Impact Assessment

Criteria	Severity			
Impact on data subject (actual or likely)	- Minimal level of data exposure (e.g. data unlikely to be exposed in the public domain, data sent in error to only a few trusted recipients such a statutory partners, or data sent to an individual with no intent to harm or publish). - Data fully recovered with no further exposure. - Access to data unlikely or deemed very difficult due to encryption or security protection. **- No detrimental impact to the data subject.**	- Low level of data exposure (e.g. exposed to limited number of people). -Data exposed to family, friends, colleagues, neighbours; but they were already aware of content. - Subject is vulnerable. - Subject may suffer damage or distress. - Subject may suffer embarrassment or reputational or financial damage.	- Wider level of data exposure (e.g. in local or regional media, or posted on an open source website with limited views). - Data exposed to family, friends, colleagues, neighbours; but they were not already aware of the content. - Subject may become victim of crime or is vulnerable. - Subject may suffer any of: identity theft, financial loss, threat to safety or threat of harm. - May cause significant impact on subject's livelihood, employment or reputation.	- Broad level of data exposure (e.g. in national media or if posted on an open source website and viewed by many). - May result in risk of serious harm or threat to life. - May result in serious injury or death. - Generic ICO advice is needed to manage and reduce the impact of the loss, on the subject.
	Data subject does not need to be informed of the data loss. ICO does not need to be notified unless the volume of data lost is significant (over 100 data subjects).	Data subject should be informed of the data loss. Data loss should be reported to the ICO if the additional 'volume' and 'sensitivity' severity scores total 4 or more.	Data subject should be informed of the data loss. Data loss should be reported to the ICO if the additional 'volume' and 'sensitivity' severity scores total 3 or more.	Data subject must be informed of the data loss. Data loss must be reported to the ICO.

Notification Matrix - Additional Factors Assessment:

If **impact assessment** = **green** or **red**: no requirement to assess the below **'sensitivity'** or **'volume'** of lost data. Follow the notification guidance above.

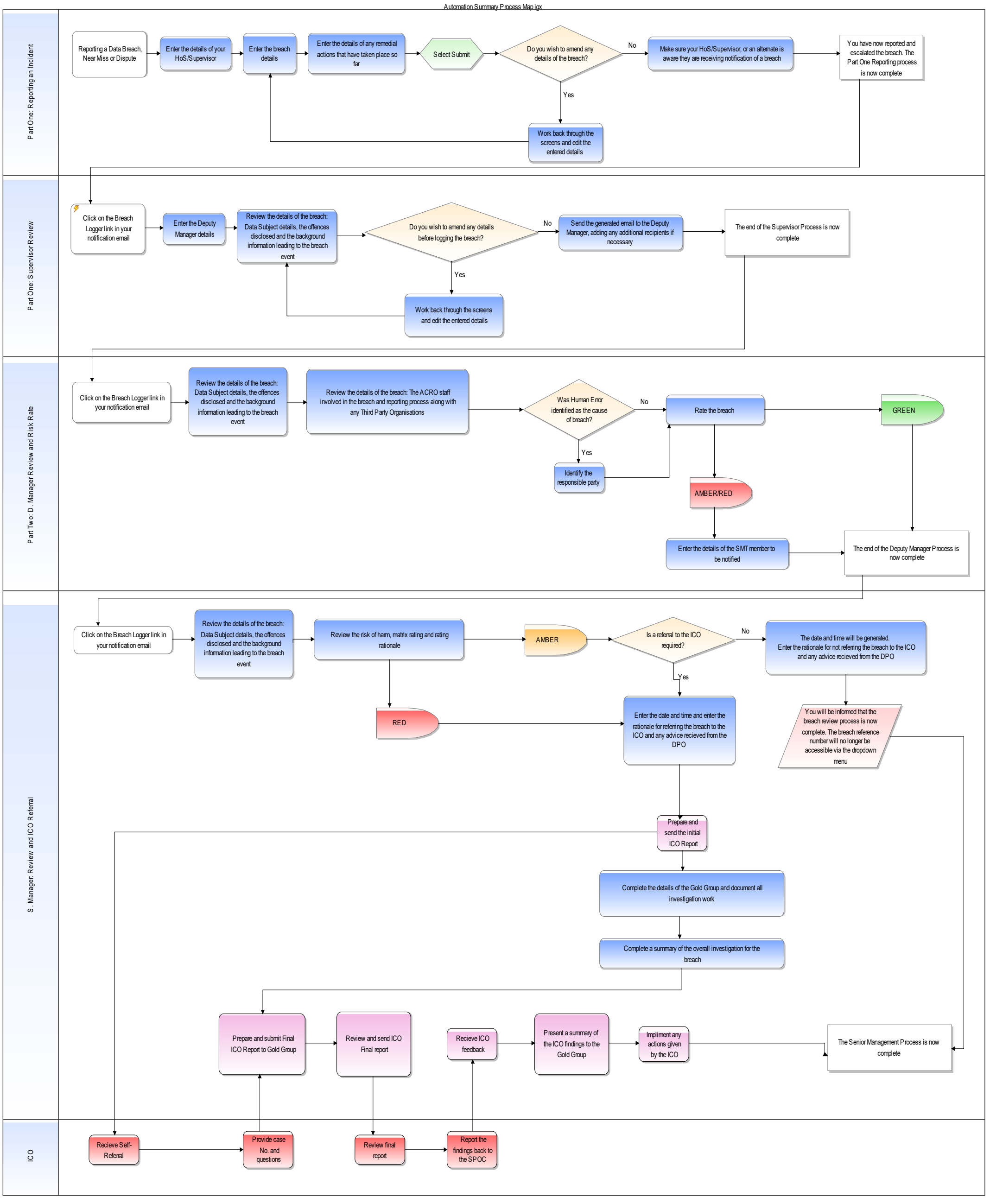
If **impact assessment** = **amber**: assess the '**sensitivity** of lost data' and '**volume** of lost data' by using the below table. For both factors identify the appropriate level of severity to provide a score for each factor.

Sensitivity of data	- Personal information. - Subject matter or the nature of the event already easily accessible in the public domain (e.g. publicised arrest). - GPMS – Protect - GSC – Official	- Sensitive personal data (e.g. offending, convictions, health / medical, safeguarding, ethnicity). - Financial information. - Information that the 'public' would consider as sensitive. - GPMS – Restricted - GSC Official Sensitive	- Very sensitive personal information (e.g. relating to serious / organised crime, sex offenders, sensitive safeguarding matters, high risk PVP, Handling Code 4 intelligence). - GPMS Confidential - GSC Official Sensitive	- Highly sensitive personal information (e.g. Covert Human Intelligence Source, witness protection, intelligence with a handling code of 5). - GPMS Secret - GSC Secret / Top Secret
	Severity score = 1	Severity score = 2	Severity score = 3	Severity score = 4
Volume of data	1- 5 data subjects (including any non police officer 3rd parties mentioned).	6 -100 data subjects (including any non police officer 3rd parties mentioned).	101 - 1000 data subjects (including any non police officer 3rd parties mentioned).	More than 1000 data subjects (including any non police officer 3rd parties mentioned).
	Severity score = 1	Severity score = 2	Severity score = 3	Severity score = 4

Add the **sensitivity + volume** scores and then return to the amber **'Impact Assessment'** boxes' to determine if notification is required.

Appendix 4 – Data Breach Process Map

Automated Data Breach Reporting: Parts 1 – 3 and ICO Actions

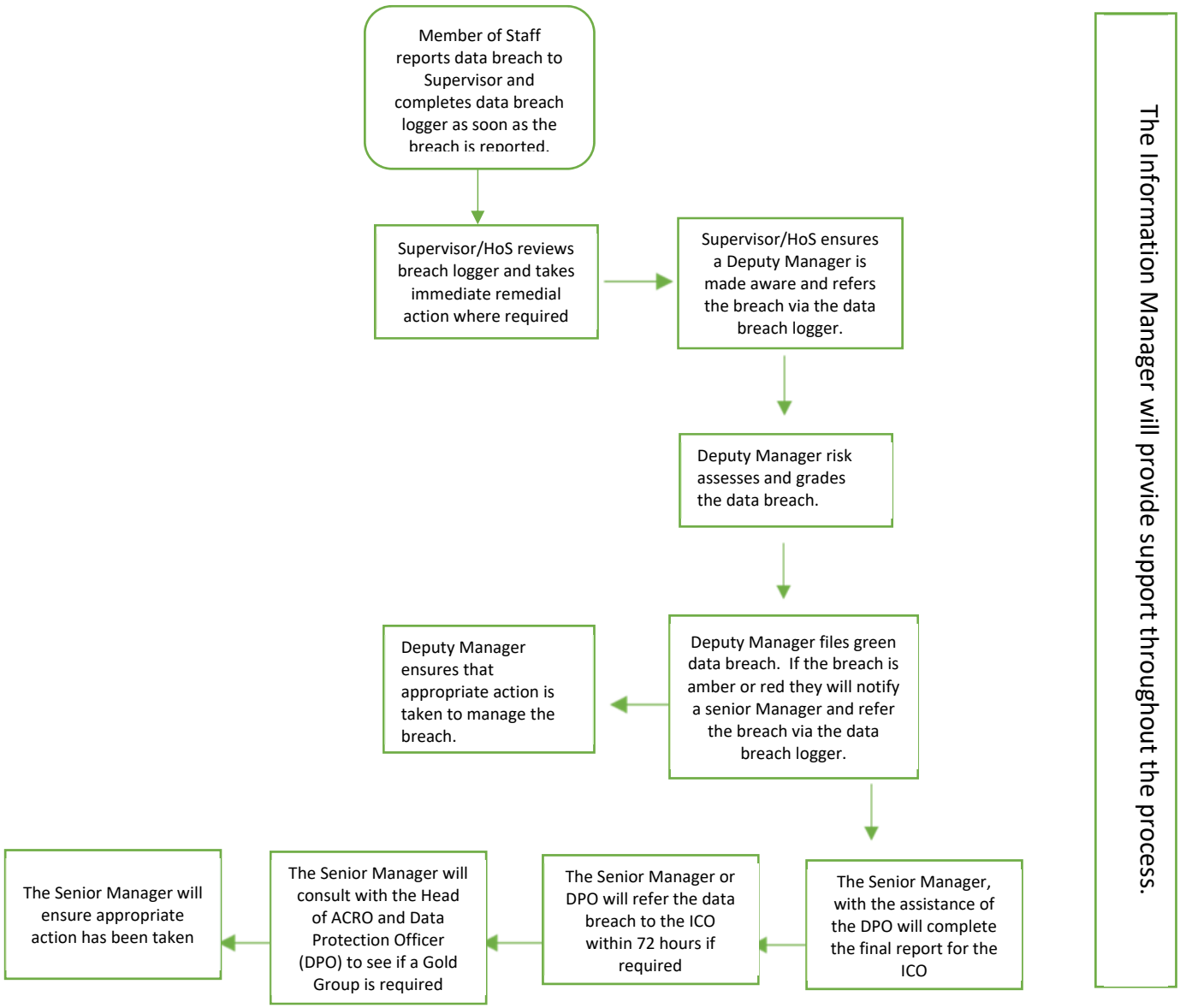


Appendix 5 – Process Maps by Role

Links:

Part One: Reporting a breach, near miss or dispute
Part One: Supervisor Review
Part Two: Deputy Manager Review and Risk Rate
Part Three: Senior Manager Review and ICO Referral

Appendix 6 – Data Breach Quick Guide – Flow Diagram



Appendix 7 – Data Breach Quick Guide

Steps 1 – 7 MUST be completed within 72 hours

1 Member of Staff reports data breach to Supervisor and completes data breach logger as soon as the breach is reported.

2 Supervisor/HoS reviews breach logger and takes immediate remedial action where required.

3 Supervisor/HoS ensures a Deputy Manager is made aware and refers the breach via the data breach logger.

4 Deputy Manager risk assesses and grades the data breach.

5 Deputy Manager ensures that appropriate action is taken to manage the breach.

6 Deputy Manager files green data breach. If the breach is amber or red they will notify a senior Manager and refer the breach via the data breach logger.

7 The Senior Manager will review all amber and red data breaches.

8 The Senior Manager will ensure appropriate action has been taken.

9 The Senior Manager will consult with the Head of ACRO and Data Protection Officer (DPO) to see if a Gold Group is required.

10 The Senior Manager or DPO will refer the data breach to the ICO within 72 hours if required. The Senior Manager, with the assistance of the DPO will complete the final report for the ICO.

11 The Information Manager will provide support throughout the process.

Appendix 8 – National guidance on notifying the ICO

Overview

This document provides guidance on a decision making process for notifying the Information Commissioner's Office (ICO) in the event of the loss, theft, unauthorised disclosure or compromise of personal data. It should be read in conjunction with the ICO's guidance on notifying data security breaches. This decision will be referred to and made by the National Police Chiefs' Council Director of Information as one of the activities that will take place in the wider management and investigation of a data loss.

'Personal data' is information which can identify a living individual. This can include information that, when combined with other readily available information, can identify a living individual.

If a loss, theft, unauthorised disclosure or compromise of non-personal data occurs then it will not be necessary to consider whether or not to notify the ICO.

Legal requirements

The use of personal data is governed by the principles set out in the Data Protection Act 2018. Under the Act all data controllers have a responsibility to ensure appropriate and proportionate security of the personal data they hold by taking 'appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'

Reporting to the ICO:

Any individual who becomes aware of the loss of their own or someone else's personal data can make a complaint directly to the Information Commissioner. Any such complaint will normally trigger an investigation by the ICO. Whether or not the incident had already been reported by the organisation involved would normally be considered by the investigators and the subsequent judgement.

'Serious' breaches are not defined by the ICO. However; the ICO Guidance advises that the following criteria should be the main factors in considering whether breaches should be reported:

- The potential detriment to individuals (the overriding consideration).
- The volume of personal data lost / released / compromised.
- The sensitivity of the data lost / released / compromised.

The following guidance provides a framework for assessing whether the ICO should be informed.

The requirements under Part 3 of the new act and GDPR (part 2) are equivalent in stating that the data controller must, on becoming aware of a breach which represents a risk to the

rights and freedoms of the data subject, report this to the ICO without undue delay and within 72 hours.

At this initial reporting stage, the data controller must state:

- the nature of the personal data breach, including where possible the categories (types) of personal data and approximate number of data subjects and personal data records concerned
- the name and contact details of the Data Protection Officer or SPOC for the breach
- the likely consequences of the breach
- remedial measures taken or proposed to address the breach and mitigate possible adverse effects

The initial breach reporting form is designed to capture these data and may be used for the initial report.

Notifying the data subject

As of May 2018, where a breach is likely to result in a **high** risk to the rights and freedoms of the data subject, the data controller shall, without undue delay, report the breach to the data subjects, with the minimum information being the standard for initial reports to the ICO (as above).

Bearing in mind that the ICO may order that the data subjects are contacted in the first two items listed below, possible exemptions to notifying them, either in full or partially exempting some of the information, are as follows:

- through technological or organisational means, or through remedial action, the data is protected in such a way that the risk is no longer likely to manifest
- the notification requires effort disproportionate to the risk (in this case, a media statement should be considered)
- where it is demonstrated to be necessary and proportionate to withhold notification to avoid prejudice to:
    - the rights and freedoms of others
    - an ongoing official or legal investigation, inquiry or procedure
    - the prevention, detection, investigation or prosecution of criminal offences, or the execution of criminal penalties
    - public and/or national security

Appendix 9 - Potential outcomes of notifying the ICO

The Information Commissioner will:

- Record the breach
- Acknowledge receipt of the notification and issue standard guidance.
- If asked, offer broad / generic advice on managing and minimising the impact of the loss on the data subject.
- Decide whether to take further investigative action by assessing the seriousness of the breach and the adequacy of any remedial action taken, to determine a course of action. The ICO's investigation could lead to one of the following courses of action:
    - Take no further action.
    - A requirement on the force to undertake a course of action to prevent further breaches.
    - Formal enforcement action turning such a requirement into a legal obligation.
    - Where there is evidence of a serious breach of the DPA, whether deliberate or negligent, the serving of a monetary penalty notice requiring the organisation to pay a monetary penalty of an amount determined by the Commissioner.

It is not the Information Commissioner's responsibility to publicise security breaches not already in the public domain or to inform any individuals affected. In so far as they arise, these are the responsibilities of ACRO. However, the ICO may recommend that the data controller make a breach public where it is clearly in the interests of the individuals concerned or if there is a strong public interest argument to do so.

Appendix 10 - Final Report to the ICO

Data Breach [Insert Ref Number]

Report to the ICO following self-referral
[Insert Date]
ACRO [Insert Portfolio]

1. Organisation Details

1.1 Is ACRO the Data Controller in respect of this breach?

1.2 If not ACRO, who is the data controller and have they been informed of the breach?

1.3 Which team in ACRO was responsible for the breach and what is their function?

1.4 Who should the ICO contact if they require further details concerning the Incident?

2. Details of the Data Protection Breach

2.1 Describe the incident in as much detail as possible

2.2 When did the incident happen?

2.3 How did the incident happen?

2.4 If there has been a delay in reporting the incident to the ICO, explain the reasons for this

2.5 What measures did ACRO have in place to prevent an incident of this nature occurring?

2.6 Provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time of the incident. Provide dates on which they were implemented

3. Personal Data Placed at Risk

3.1 What personal data has been placed at risk? Specify if any financial or sensitive personal data has been affected and provide details of the extent.

3.2 How many individuals have been affected?

3.3 Are the affected individuals aware that the incident has occurred?

3.4 What are the potential consequences and adverse effects on those individuals?

4. Containment and Recovery

4.1 Has ACRO taken any action to minimise/mitigate the effect on the affected individuals? If so provide details.

4.2 Has the data placed at risk now been recovered? If so provide details of how and when this occurred.

4.3 What steps has ACRO taken to prevent a recurrence of this incident?

4.4 Have the data subjects made any specific requests or made a complaint?

5. Training and Guidance

5.1 Does ACRO provide its staff with training on the requirements of the Data Protection Act? If so, provide any extracts relevant to this incident. ACRO adheres to its own Data Protection Breach guidance and Standard Operating Procedure:

5.2 Confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?

6. Previous Contact with the ICO

6.1 Have you reported any previous incidents to the ICO in the last two years?

6.2 If the answer to the above question is yes, provide the ICO reference number.

7. Miscellaneous

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

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

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

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

8. ICO Questions

8.1 If the ICO has asked any questions in relation to this breach please add them here.

Appendix 11 HR Guidance for Managing Performance

Guidance for managing data breaches in accordance with the ACRO data breach, managing performance and probationary period for police staff policies

Created by ACRO HR but guidance for all ACRO departments

1. Taking relevant action in accordance with policy

1.1 In order to ensure the organisation take a fair and consistent approach to data breaches, this document provides HR guidance to managers to assist them in managing data breaches in accordance with the ACRO data breach, managing performance and 33013 probationary period for police staff policies.

1.2 It is imperative all ACRO staff adhere to legislation and local policies and practices as these are in place to minimise the risk of a data breach.

1.3 As stated on the role profile, there is an expectation that each member of staff will "keep up to date with changes in legislation, local procedures and/or policies that affect working practices and the use of police databases or systems (including European or International requirements where appropriate)."

1.4 It is important to appreciate and acknowledge that there could be an element of human error but it is imperative that staff understand the potential of a data breach if care is not taken.

2. Factors to consider when determining the action to take

2.1 If a data breach is identified, the following factors should be taken into consideration, for each member of staff involved in the data breach, when determining what action should be taken.

2.2 If the member of staff has not followed the relevant process (at the time of the data breach), especially if the breach could have been prevented had they done so, then

action should be taken under the managing performance policy or 33013 probationary period for police staff policy (if staff are still within their probationary period).

2.3 It is important to ascertain whether this is the first data breach that the member of staff has been involved with or if the member of staff has been involved in a series of data breaches. If this is the first data breach that the member of staff has been involved with then the other factors detailed in this guidance document should be taken into account when determining the action to be taken. If, however, the member of staff has been involved in a series of data breaches (of a similar nature)

then relevant action should be taken under the managing performance policy or 33013 probationary period for police staff policy (if staff are still within their probationary period).

2.3.1 It is imperative that the seriousness of the breach is considered when determining the action to be taken. For example:
- How many data subjects were impacted by the breach?

- What risk is posed to the data subjects as a result of the breach?

- What is the reputational impact for ACRO as a result of the breach?

- What is the impact on policing in general (were other forces involved in the breach?

If the breach was graded red on the risk rating matrix/impact assessment then relevant action should be taken under the managing performance policy or 33013 probationary period for police staff policy (if staff are still within their probationary period).

2.4 The time period between the member of staff taking action and the date that the data breach came to notice should be considered as this may have impact on the processes and policies that were relevant at that time and potentially the action that the member of staff took as a result. For example:
- Is it a historic breach?

- Was it the member of staff who raised the breach and/or did they know the breach had taken place or was this picked up and raised by another member of staff?

2.5 It is important to take into account whether the member of staff has received the relevant training for their role. For example:
- Has the member of staff received training in relation to that work stream and is their working knowledge and experience up to date?

- Is the member of staff's PNC training and knowledge up to date?

2.6 It can be helpful to establish whether evidence can be gathered via the relevant systems used in the process, for example can a GSA or PNC report be generated (if necessary) to ascertain exactly what action was taken by the member of staff and if so, did the member of staff act in accordance with the system and process guidelines?

2.7 Consideration should be given as to whether there are any other factors that need to be taken into account. For example:
- Is there a possible underlying medical condition or disability and therefore are there any reasonable adjustments that need to be implemented prior to action being taken under the relevant policy?
- Is Occupational Health advice required before determining the action to be taken?
- Are there any personal circumstances that need to be taken into account when determining the action to be taken?
- Has the member of staff got the relevant skills and behaviours to undertake their role?

3. Organisational Learning

3.1 Consideration should be given as to whether there is any organisational learning that needs to be considered and any remedial measures that have been identified and actioned as a result of the data breach, for example:
- Could an IT fix could be proposed in order to prevent or minimise the risk of similar data breaches in the future?

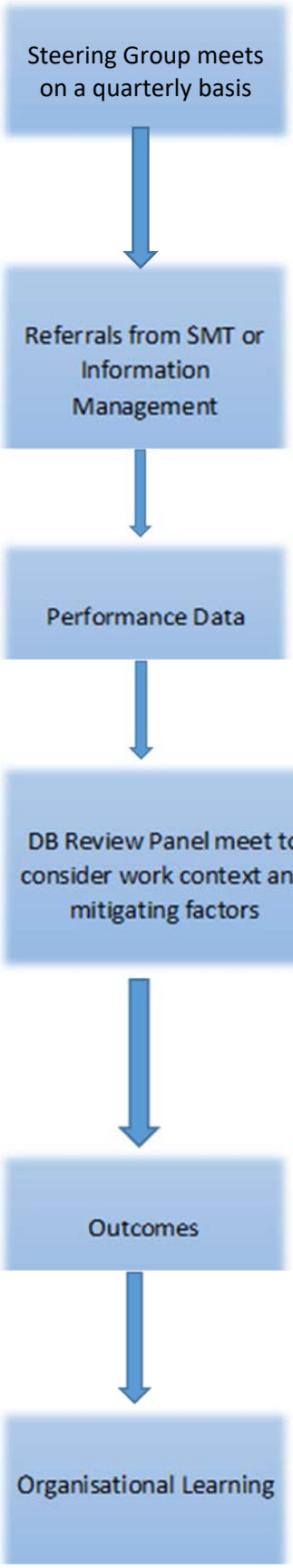
- Is refresher data breach training required?

- Is support/guidance/training required from the ACRO Systems Trainer?

- Has the breach prompted a change in process?

- Has the breach identified a training need for specific roles/team/business area?

Appendix 12 – Steering Group Guide



The Steering group, Chaired by the DPO or Information Manager, will meet on a quarterly basis. Regular attendees will include the SMT for National Services, International Services and Projects & Intelligence. An HR Manager or advisor will attend to advise on HR policy. Other SMT may be invited if staff in their business areas require discussion.

A referral to the Steering Group can come from Information Management, or a Senior/Deputy Manager who may have concerns about an individual who has made a significant breach, or multiple breaches.

In advance of the meeting the Information Manager will provide attendees with performance data about any staff member to be discussed

The Steering Group will consider all available information, including the following;

- The volume of work undertaken by the individual
- The training provided to the individual
- Whether the individual has been spoken to previously about breaches
- The hours and pattern worked and output
- What processes they are undertaking
- Any mitigating factors which may help to explain

Outcomes could include NFA, management advice, training or more formal action in line with the appropriate procedure. Decisions are to be made in collaboration with the HR team and recorded to ensure fairness and consistency.

Outcomes from the Data Breach Steering Group should be anonymised and high level data provided to ensure staff awareness of breaches. This will seek to inform organisational learning and help to prevent further breaches.