Information Security Document

Corrective And Preventative Action (CAPA) Procedure (ISO27001)

Version 7.0

Version History			
Version	**Date**	**Detail**	**Author**
1.0	27/03/2013	Approved by Information Governance Group	Jo White
2.0	30/08/2013	Reviewed by Information Governance Group. 5.2 expanded on scheduled audits and IS reviews.	Jo White
3.0	13/04/2015	Reviewed by Information Governance Group.	Jo White
4.0	09/05/2016	Reviewed by Information Governance Group.	Jo White
5.0	12/06/2017	Reviewed by Information Governance Group.	Jo White
6.0	06/08/2018	Reviewed by Information Governance Group. Change from EDRM spreadsheet to workflow.	Jo White
7.0	08/10/2019	Reviewed by Information Governance Group. No changes.	Jo White

1 Purpose

1.1 The purpose of this procedure is to describe the CAPA ('Corrective Action and Preventive Action') process for handling non-conformities.

2 Distribution

2.1 This procedure is distributed to all Employees and associated Contractors or third parties as all individuals have a responsibility for continual improvement.

3 Responsibility

3.1 The Information Security Manager is responsible for the maintenance and distribution of this procedure.

4 Monitoring and Review

4.1 This procedure shall be continually monitored and shall be subject to a regular review which shall take place annually, or when a significant change is made to the systems, people or processes related to this procedure.

5 Process Details

5.1 Handling of Non-conformities

Where non-conformities are identified through the Management System or through monitoring and review, Derbyshire County Council shall employ CAPA as detailed in Section 5.2, to mitigate their impact.

5.2 CAPA

CAPA focuses on the systematic investigation of discrepancies (failures and/or deviations) in an attempt to prevent their recurrence (for Corrective Action) or prevent from occurrence (for Preventive Action). To ensure that Corrective Actions and Preventive Actions are effective, the systematic investigation of the failure incidence is pivotal in identifying the Corrective Actions and Preventive Actions undertaken. CAPA is part of the overall Management System.

CAPA shall be used to identify, correct and eliminate the cause of potential and actual non-conformance, minimising the risk of poor quality and providing continuous improvement. When a discrepancy arises, through scheduled audits, information security reviews, feedback and from other non-conformities identified through the group, the Corrective and Preventative (CAPA) Investigation and Response Form shall be used. This form is used to:

- Describe the discrepancy;
- Investigate the discrepancy;
- Investigate and analyse the root cause;

- Detail the Corrective Actions to take;
- Detail the Preventative Actions to take; and
- Verify the Effectiveness of the Corrective Actions and Preventive Actions taken.

If through investigations actions are to be taken, these could be either Corrective or Preventative Actions and are described in Sections 6.3 and 6.4.

If scheduled internal Audits find a non-conformance, this will be discussed and agreed with the relevant Manager or Strategic Director/Director at the conclusion of the review. The nature of the non-conformance and associated recommendation will then be incorporated within the Audit Services Memorandum and Action Plan issued to the Manager or Strategic Director/Director for details on how the recommendations will be addressed and actioned. It is the responsibility of Senior Management from the relevant department for implementing corrective actions to address the recommendations made and agreed by Audit Services.

Following the issue of the Audit Services memorandum and action plan it is important that, where possible, the 'root cause' is identified and investigated to prevent reoccurrence in the future. Departmental Information Governance Group (IGG) representatives are responsible for identifying the 'root cause' of audit findings reported within their respective departments and taking action to address the issue. Details of the action taken to correct the non-conformity should be recorded within the ISO27001 Record Log in EDRM under the heading 'Root Cause'. A standard item is included on the IGG agenda to enable the monitoring of 'root cause' analysis.

To provide additional transparency to the Information Governance Group of non-conformities identified across the Authority all such findings will be recorded by the 'ISO27001 Record Log' workflow held within the Derbyshire County Council's Electronic Document Record Management system (EDRM). The non-conformities within the workflow are categorised by Department. Access to the information within the workflow and will be provided on a Departmental basis to the representatives at the Information Governance Group. Departmental representatives are expected to add comments regarding non-conformances and root cause analysis specific to their Department. The Information Security Team will have view access across all Departmental non-conformities and also the ability to add comments.

It is the responsibility of Audit Services to maintain the information within the 'ISO27001 Record Log' workflow at the point when each Audit Services Memorandum is issued. The monthly Audit Services' report to the Information Governance Group will provide a summary of the recurrent non-conformities across all Departments.

6.3 Corrective Action

Where an issue of nonconformance is identified Derbyshire County Council shall:

- Ensure that any remedial action is taken to deal with the immediate issue identified. For example, the Employee's training Records that are not up to date are updated; and
- Then through the investigation and analysis of the root cause, understand the cause of the deviation and if applicable, through the Change Management Procedure request any changes to potentially prevent recurrence of a similar problem.

6.4 Future Action

Derbyshire County Council uses a proactive methodology to determine potential discrepancies/non-conformities before they occur and if applicable takes action through the Change Management Procedure to eradicate them. This shall be through:

- Preventive education and training;
- Management review; and
- Risk Assessments (i.e. as described in the Information Security Policy).

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.