Derbyshire County Council ISO27001 Scope

1 Version History, details and author

1.0	01/08/2012	Approved by Information Governance Group	Jo White
2.0	27/03/2013	Reviewed by Information Governance Group to expand on scope areas and processes	Jo White
3.0	30/08/2013	Reviewed by Information Governance Group. Several Asset Owners have changed.	Jo White
4.0	10/08/2015	Reviewed by Information Governance Group. Incorporation of definitions of internal and external stakeholders.	Jo White
5.0	12/09/2016	Reviewed by Information Governance Group. Coroners added and Risk Owners updated. Council business activities updated.	Jo White
6.0	11/06/2018	Reviewed by Information Governance Group. Department names and Risk Owners updated.	Jo White
7.0	08/07/2019	Reviewed by Information Governance Group. Changes to department names, risk owners and departmental statistics.	Jo White
8.0	16/06/2020	Reviewed by Information Governance Group. Changes to department names, risk owners and departmental statistics.	Jo White
9.0	06/07/2021	Reviewed by Information Governance Group. Changes to department names, risk owners and departmental statistics.	Jo White
10.0	09/08/2022	Reviewed by Information Governance Group. Changes to department names, risk owners and departmental statistics.	Jo White
11.0	01/08/2023	Reviewed by Information Governance Group. Changes to department names and risk owners.	Jo White
12.0	10/09/2024	Reviewed by Information Governance Group. Changes to risk owners,	Jo Williams

2 Introduction

This document describes the scope of the Council's Information Security Management System (ISMS) and how information assets are protected from influences which are outside of the ISMS scope.

The Council's ISMS functions in accordance with the ISO27001:2022 standard and all legal, regulatory and statutory requirements as identified below:

- The Data Protection Act (2018)
- UK General Data Protection Regulation
- The Freedom of Information Act (2000)
- Environmental Information Regulations (2004)
- The Computer Misuse Act (1990)
- The Human Rights Act (1998)
- The Copyright, Designs and Patents Act (1988).
- The Regulation of Investigatory Powers Act (2000)
- The Electronic Communications Act (2000)
- Privacy and Electronic Communications Regulations (2003)

Also included within this document:

- A written scope defining company core business;
- Boundaries of scope;
- Geographical locations;
- Organisational employee structure; and
- Responsibilities and any other appropriate information.

3 Information Security Management System Scope

The Information Security Management System of this Business Management System is based on BS EN ISO27001:2022.

The scope of the certified Information Security Management System is for:

"The protection of all information and data assets for the delivery of all Council functions, services and activities - excluding schools. The assets protected are physical locations, hardcopy data, electronic data, Council records, policies and procedures, software and licences and physical IT hardware. The boundaries of the Information Security Management System are the physical locations, authorised mobile workers and the endpoints of the organisational network. Supporting technology includes server platforms, network devices and organisational networks within the control of Derbyshire County Council, in accordance with Statement of Applicability Ver 5"

3.1 Within Scope

Excluding schools, the Information Security Management System applies to all functions, services, activities and data information assets of Derbyshire County Council.

3.2 Out of Scope

Schools and associated school maintained premises and resources are managed autonomously. Schools are beyond the scope of the Council's ISMS however, the Council provides key services to schools – many of which, schools may opt in or out of. Workplaces in buildings owned by third parties that Council staff work from.

4 ISMS Scope Boundaries

The relationship between the Council's internal business/services within the ISMS scope and those which are out of the ISMS scope are identified below. Council services and activities

within scope have been identified where there is a risk to information beyond the Council's business end-points.

WITHIN THE ISMS SCOPE – COUNCIL SERVICES AND ACTIVITIES

- Adult Social Care and Health services
- Audit Services
- Call Derbyshire (call centre)
- Children's Services
- Computer and Internet use logs
- Coroners
- Corporate records
- Council Employee information
- Council premises and facilities
- Council public facing websites
- Derbyshire Business Centre
- Derbyshire Record Office
- Economy, Regeneration and Planning Services
- Finance
- Freedom Of Information requests
- Highways and Transport Services
- Hubs
- Legal services
- Libraries & Heritage
- Pensions
- Property Services
- Registrars (Birth deaths and marriages)
- School admissions and referrals
- School Support services
- Subject access requests
- Trading Standards
- Waste and Environment Services

OUT OF THE ISMS SCOPE – EXTERNAL PARTY ACCESS TO INFORMATION & SERVICES

- Borough and District Councils
- The Coroner and Assistant Coroners
- Court Services
- Diocese of Derby
- Government Agencies
- Magistrates Courts
- NHS
- The Police
- The Public
- Schools
- Third Parties

EXTERNALLY CONTRACTED SERVICES AND SUPPLIERS

- IT Solutions, services and maintenance
- Disposals
- Building contractors
- Agency workers
- Cleaners
- Offsite storage
- Personal (medical) aides
- Environmental services
- Waste
- Highways
- School and Social Care transport
- Public Transport
- Nursing Homes
- Individual Agencies

In delivering these services, the Council relies on many third party suppliers who are contracted to provide solutions and services which may store, process and generate Council information or who may have access to Council information. The Council is also required to share information with government and other outside agencies due to legal, regulatory, statutory or business requirements. The Council protects the confidentiality, integrity and availability of information which is held in locations by suppliers and other agencies that are outside of the Council's ISMS scope by ensuring robust procurement processes, contractual and information sharing agreements are in place.

5 Company Stakeholders

Derbyshire County Council delivers services for people of all ages in every community across the county. Many, but not all, of these services are required due to legal, statutory or regulatory requirements. Much of the information and data which is held and/or generated by delivering these services is subject to protection under the UK General Data Protection Regulation and the Data Protection Act 2018 and the Council works to ensure that this information is protected at all times. The Council's information asset risk management strategy has identified and appointed information asset Risk Owners from all departments. Risks to Information assets are recorded in departmental Asset Registers and managed under the Council's Information Security Management System (ISMS).

6 Key Business Risk Owners and Departments covered

Neil Brailsford – Adult Social Care and Health

Service Manager, Adult Social Care and Health.
Responsible for Adult Social Care and Health activity other than finance, client data held in electronic and paper form and other non-financial systems.

Martin Stone – Children's Services

Team Manager, Corporate Services & Transformation, Digital Services.
Responsible for Management Information, ICT and Information Governance for Children's Services staff.

Steve Allen – PLACE Trading Standards

Head of Trading Standards, PLACE.
Responsible for Trading Standards staff and IT systems. Also responsible for hardcopy case files and evidence files.

Michelle Parker, Robert Clayton – PLACE Libraries

Head and Interim Head of Libraries & Heritage. PLACE.
Responsible for libraries, library management system and user data. Also responsible for museum artifacts, Derbyshire Record office cataloguing system, physical archives, book stocks and Arts website.

James Rhodes – Corporate Services & Transformation, Strategy & Policy

Assistant Director Strategy & Policy, Corporate Services & Transformation.
Responsible for electronically held data such as systems used by Public Relations, Complaints, Citizens personal data, Members' Casework system and Communications personnel.

Steve Harrison – Corporate Services & Transformation, Derbyshire Business Centre

Business Services Manager, Corporate Services & Transformation.
Responsible for the Derbyshire Business Centre which prints out the majority of the Council's mailings, payslips, staff rotas, P60s and pension files. Also responsible for the delivery and dispatch of post, photocopying, press equipment and multi-function devices.

Michael Crawford – Corporate Services & Transformation, Finance

Head of Exchequer Service, Finance, Corporate Services & Transformation.
Responsible for all corporate financial systems, personal data held electronically on those system, paper based pension files and other paper based financial records including invoicing. Also responsible for risk and insurance.

Janet Scholes – Corporate Services & Transformation, Property

Director of Property, Corporate Services & Transformation.
Responsible for all council physical premises, asset management and job management systems, various files and databases used by Property Services and paper files relating to drawings, invoices and planning.

Mark Smith – PLACE, Records Office

Corporate Records Manager, PLACE.
Responsible for hardcopy offsite storage documents, records management within the Electronic Document and Records Management system, records management procedural framework.

Rob Brittan – PLACE, Emergency Planning

Functional Lead Emergency Planning, PLACE.
Responsible for the Council's Business Continuity and Emergency plans and associated underpinning data. Also responsible for the Council's security key system.

Julian Gould, Joe Battye, Claire Brailsford – PLACE

Directors of Highways, Economy & Regeneration, Environment & Transport respectively.
Responsible for PLACE department's mobile devices, specialist technical equipment, protective monitoring systems, departmental ICT systems, personnel, properties and the Council's vehicle fleet.

Lee Gregory – Corporate Services & Transformation, HR

Head of HR Services Corporate Services & Transformation.

Responsible for HR System, HR personnel files, medical records, accident/assault records and corporate learning and development.

Helen Barrington – Corporate Services & Transformation, Legal Services

Director Legal Services, Corporate Services & Transformation.
Responsible for Legal Services IT System and associated paper files, Council minutes and reports, general office personal information and financial details and the Registration Service.

Ellie Houlston – Adult Social Care & Health, Public Health

Director of Public Health, Adult Social Care and Health.
Responsible for Public Health staff, Public Health and Knowledge Services Teams personnel information. Also responsible for Public Health Births and Mortality files, Public Health Hospital Episode Statistics data, Derbyshire Health United Care Home and Rightcare Contacts information and other data held and shared from and to the NHS and commissioned providers.

Leonardo Tantari – Corporate Services & Transformation, Digital Services

Director of Digital Services, Corporate Services & Transformation.
Responsible for the Corporate Service Desk, the Council's PC and Laptop estate, equipment commissioning and disposals, the Council's Data Centres, servers, networks, telephony, offsite storage for electronic data, support and maintenance contracts for equipment, the Council's technical specialists, internet, email, departmental applications, security incident management and business continuity.

7 Company Structure

The company structure can be observed in Appendix 1

Derbyshire County Council employs a workforce of over 16,000 to collect and process information to enable the delivery of the above services. The Council is also responsible for the employment and pension information for both the current workforce and retired employees.

8 Geographical and Physical

There are approximately 200 key office locations and Derbyshire County Council employees can also work from home or as mobile workers.

The list below identifies the sites, locations and asset types:

Head Office - County Hall, Matlock - Main Data Centre, all office equipment and core information assets.
Derbyshire Record Office – Matlock - Office equipment and information assets.
The Quad – Chesterfield - Office equipment and information assets
The Hub – South Normanton - Office equipment and information assets.
3 Business Units - Chesterfield, Denby, Doveholes - Office equipment and information assets.
9 Highways/Street Lighting/Transport Depots - Various locations - Office equipment and information assets.
12 Council Social Care Office Bases - Various locations - Office equipment and information assets.
39 Children and Family Centres/Homes - Various locations - Office equipment and information assets.
45 Branch Libraries - Various locations - Office equipment and information assets.
20 Registered Care Homes - Various locations - Office equipment and information assets.

22 Day Care Services - Various locations - Office equipment and information assets
7 Countryside Sites/Visitor Centres - Various locations - Office equipment
Home & Mobile workers - Various locations - Paper information assets and Digital information assets on all Digital Devices.
Markham Vale Environment Centre – Chesterfield - Office equipment and information assets.

Breakdown of Council business activities and end-points:

- Supports over 400 schools.
- Run 12 children's centres and support day nurseries, pre-schools, out of school clubs, creches, holiday scheme and childminders providing early years support.
- Support foster carers, runs children's homes, family support centres and residential respite care homes.
- Help over 16,000 vulnerable and older people to live at home through directly provided services, housing-related support and services through the independent and voluntary sector.
- Support over 250people in residential and nursing care.
- Assist over 2,000people to arrange their own services through Direct Payments.
- Maintain over 3k miles of roads plus bridges, footbridges, public rights of way, over 600 miles of retaining wall and over 89k street lights.
- Operate a gritting route that covers 50% of our roads each year.
- Run 45 branch libraries, 2 mobile libraries, 1 museum and the Record office .
- Manage 4 country parks, 5 visitor centres, manage 120 countryside sites.
- Run 9 household waste recycling centres and dispose of more than 389,000 tonnes of waste each year.
- Manage a network of over 200 miles of cycleways and greenways.
- Supports over 100 School Crossing Patrol sites across the County.
- Have over 900 businesses that are members of our Trusted Trader scheme.
- Respond to complaints, enquiries and requests for advice from the public and businesses.
- Manage over 50,000 enquiries and referrals annually through Call Derbyshire, the Council's contact centre.
- Manage a portfolio of 18 websites; including Derbyshire.gov.uk.
- Respond to over 80 emergency planning incidents each year.
- Commissioning Health Visiting service making antenatal visits and baby and toddler reviews.
- Commissioned School Nursing service undertaking school entry health reviews, Year 6 reviews, hearing screenings and vision screenings.
- Delivery of the National Child Measurement Programme (NCMP) measuring 4-5 and 10-11 year olds.
- Substance Misuse treatment and recovery services.
- Exercise Referral Schemes.

- Funded walking for Health programme.
- Stop Smoking Commissioned services.
- Feeding Derbyshire Scheme.
- Commissioned Falls prevention programme.
- Manage over 40K Service Requests and Incidents annually through the Digital Services Service Desk.
- Actively maintain over 99.98% availability of the Council's Digital Infrastructure.

9 Information Security Objectives

Business Objectives are documented in the Corporate Business Plan.

In addition to Business Objectives, Information Security Objectives are also set. These are discussed in the Information Governance Group Terms of Reference.

Terms of Reference

The Council's Information Governance Group manage and review the Council's Information Security Management System (ISMS) to ensure its continuing suitability, adequacy and effectiveness. This shall include identifying opportunities for continuous improvement and the need for change.

Help to ensure there is an appropriate, comprehensive information governance framework is in place throughout the organisation, in line with national and regional standards.

Review, monitor, publicise and ensure the continuous development of effective information security related policies, procedures and guidelines.

Ensure information security communications and awareness training is effective.

Ensure the Council remains compliant with information security legislation, regulations, best practice and contractual obligations.

Help to ensure the Council's systems and processes are secure, fit for purpose and the Council is able to work collaboratively with third parties and exchange information with those third parties securely.

To facilitate safe and secure communication, collaboration and information sharing with third parties to support the Council's service objectives.

Raise awareness of issues from the National Cyber Security Centre (NCSC) to build and improve capability for the Council to manage cyber security threats and incidents effectively.

To seek continuous cultural change within the Council, such that keeping personal information safe but sharing information where it is legal and appropriate to do so, is embedded in everything the Council does.

Role of the Group:

1. To develop the Council's Information Governance work programme to establish good practice, promote a culture of information security awareness and ensure improvements to existing processes are implemented.
2. To ensure that an appropriate comprehensive Information Governance framework and systems are in place throughout the Council in line with national standards.
3. To inform and review the Council's management and accountability arrangements for Information Governance.
4. To validate reviews of existing information security policies, procedures and guidelines and develop responses to new threats as they emerge.
5. To develop and maintain an Information Security Management System which conforms to the ISO 27001 standard.
6. To raise concerns, risks and incidents associated with information security and to ensure that 'lessons learned' from data breaches are implemented within the Council.
7. When information security instances arise, help to ensure the organisation responds effectively to these instances and help to ensure management action takes place to protect the Council's information security arrangements.
8. To establish and support effective communication to ensure that the Council's approach to information handling is communicated to all Derbyshire County Council employees, elected members, partner agencies, contractors and vendors with access to Council systems and made available to the public.
9. To promote best practice in safe and secure information sharing with third parties in support of service objectives.
10. To coordinate the activities of employees given data protection, confidentiality, security, information quality, records management and Freedom of Information responsibilities.
11. To offer support, advice and guidance to the Caldicott Function and Data Protection programme within the Council.
12. To monitor the Council's information handling activities to ensure compliance with law and guidance.
13. To ensure that security awareness training is made available by the Council and is taken up by staff as necessary to support their role.
14. To provide a focal point for the resolution and/or discussion of Information Governance issues.
15. To receive reports from the Information Implementation group
16. To assist the Council in compliance with the UK General Data Protection Regulations (UK GDPR)
17. To review Data Protection Impact Assessment process and seek to ensure the Council is applying a consistent approach.

Membership:

The IGG Chair will decide the number of places to be offered to each Information Risk Owner (IRO). The IRO will decide whether to attend IGG or to delegate to as many registered Information Asset Owners (IAO) as are needed to fill their allocation of places, plus deputies when the IAO is absent.

The current membership of the Information Governance Group (IGG) is

- Director of Digital Services (Chair)
- The Council's Data Protection Officer (Vice-Chair)
- The Council's Risk Manager or nominee
- The Council's Records Manager
- One senior representative from each service Department

- One senior representative from Legal Services, Audit Services, Communications, Property Services, Digital Services and HR Services

Members of the Group will:

- Ensure engagement and awareness of the work of the Information Governance Group with Executive Directors/Directors and senior management team
- Reflect the views of their department/function and contribute to decision making on action plans, policy developments and service delivery relating to Information Governance
- Consult with their department/function and contribute views based up on implications for implementation of Information Governance requirements from their departmental/function service delivery perspective
- Keep departments/functions informed on priorities, developments and decisions
- Ensure communication mechanisms are in place within their departments/functions to ensure information and actions are cascaded throughout the Council
- Implement any agreed actions ensuring consistency of approach throughout the Council
- Influence actions, behaviours and approaches and promote issues regarding Information Governance and best practice for sharing and collaboration with third parties, within their department/function
- Maintain sensitivity, confidentiality and diplomacy with regard to any proposals

10 Organisation and Structure:

The IGG Chair will report data and security issues to the Council's Corporate Management Team (CMT) as appropriate. This will be on a 6 monthly basis.

In addition the Council's Data Protection Officer will also report to CMT as they think appropriate.

Members of the Group are responsible for ensuring that issues raised are reported to their respective management teams.

Sub-groups:

Any member of IGG has the right to propose formation of a sub-group or working party. Draft terms of reference should be appended to any such proposal, including a duty to report back to IGG. IGG will reserve the right to amend or withdraw the terms of reference for any group set up in this way.

The Information Implementation Group (IIG) and the GDPR Group are currently identified as sub-groups of the IGG. The IIG will focus on responsiveness issues such as consistency in FOI and SAR responses. The GDPR Group will focus on preparedness and accountability in the field of data protection.

11 Responsibilities for Information Security

Derbyshire County Council specifically reviews Information Security in a dedicated Forum. The following Employees constitute the forum:

- Director of Digital Services (Chair);
- Data Protection Officer

- Information Security & Governance Manager;
- Adult Social Care and Health Performance;
- Information Children and Younger Adults';
- Service Relationship Manager, PLACE;
- Corporate Risk Manager
- Corporate Records Manager;
- Senior Policy and Research Manager Chief Executives;
- Group Manager Property Services;
- Assistant Director Digital Services
- HR Management Information Lead;
- Senior Solicitor Legal Services;
- Principal Auditor.

All information security related issues and incidents are reported to the Information Governance Group as part of the Agenda and policies and procedures support incident reporting and management.

12 Monitoring and Review

This document shall be continually monitored and shall be subject to a regular review which shall take place annually, or when a significant change is made.