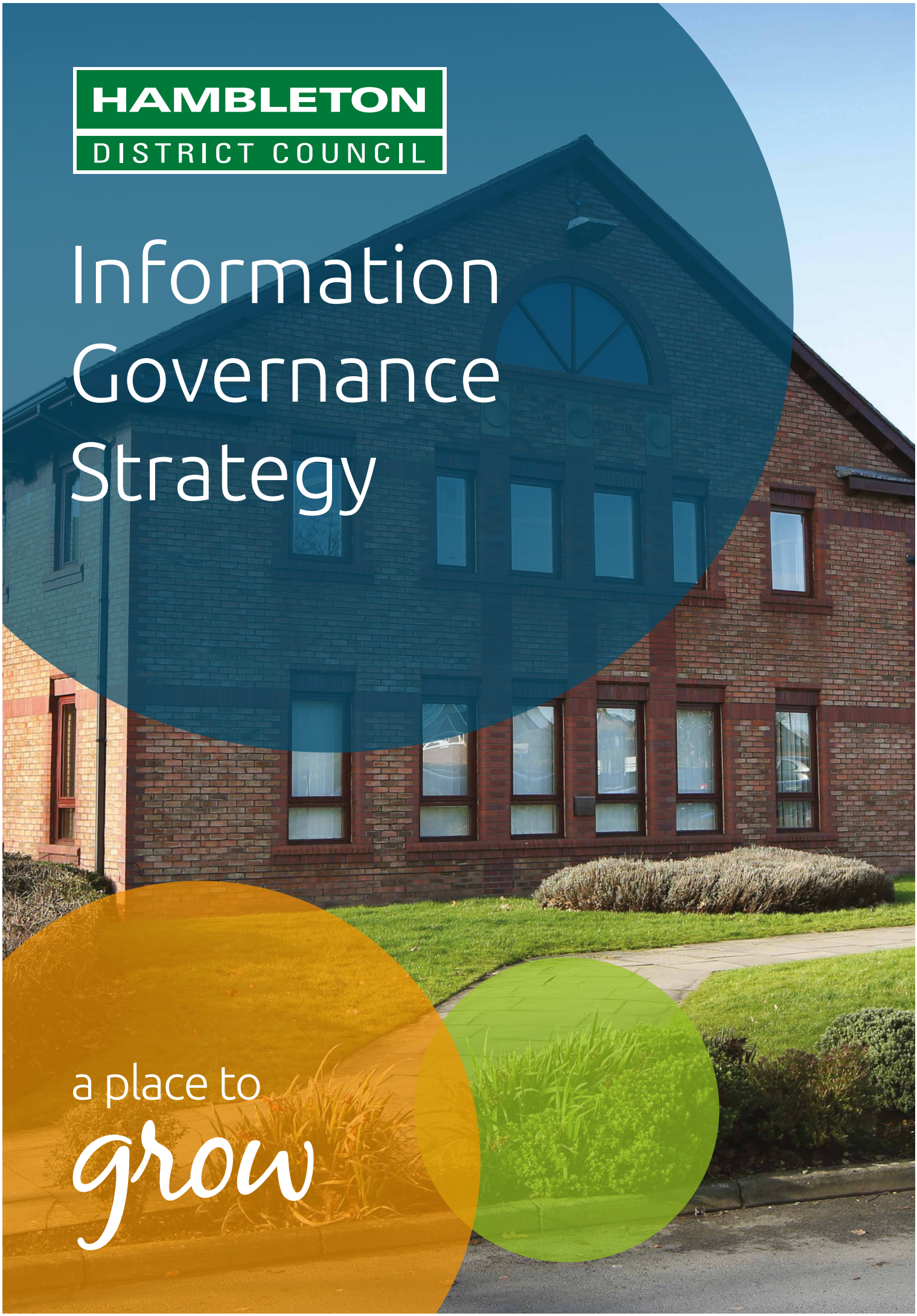
HAMBLETON
DISTRICT COUNCIL

Information Governance Strategy



a place to *grow*

Contents

Version:	1.0
Publication date:	3.10.19
Policy review date:	3.10.20

Introduction and scope

In May 2018 the UK's existing data protection framework was replaced by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. As part of Hambleton District Council's compliance with this new legislative framework it has introduced a new information governance policy framework.

This document outlines the council's overarching information governance strategic objectives, examines information governance risks, and assigns roles and responsibilities to council officers.

The Information Governance Strategy is the council's principle information governance policy document and sits above all other policies in the policy framework. The council's information governance policy framework can be found in Appendix One of this document. For clarity the policies in this framework covers:

- Information Access and Transparency Policy
  - Local Government Transparency Responsibilities
  - Publication Scheme
  - FOI and EIR Requests
  - Re-use of Public Sector Information (RoPSI)
  - Internal Reviews
  - Appendix One: List of Transparency Responsibilities
  - Appendix Two: FOI Charging Structure
  - Appendix Three: EIR Charging Structure
  - Appendix Four: Information Governance Appeals Notice
- Data Protection Rights Policy
  - Subject Access Requests
  - Rights to Erasure, Rectification, and Restriction
  - Right to be Informed of and Object to Automated Decision Making Technology
  - Right to Data Portability
  - Access to Information by Third Parties about Deceased Individuals
  - Accepting Requests by Third Parties on behalf of Data Subjects
  - Data Protection Complaints
  - Appendix One: DPA Charging Structure
  - Appendix Two: Data Protection Rights Extension Authorisation Process Map
  - Appendix Three: Information Governance Appeals Notice
- Personal Privacy Policy
  - Privacy Notices
  - Consent Forms

- Information Sharing
- Third Party Data Processors
- Data Protection Impact Assessments
- Training
- Automated Decision Making Technology Safeguards

- Information Management Policy
  - Data Quality
  - Information Asset Management
  - Records of Processing (Article 30 obligations)
  - Retention and Destruction of Records
  - Case Management
  - De-identification and Re-identification of Personal Data
- Information Security Overview
  - ISO:27001 Compliance
  - Information Security Assurance Statements
  - Information Security Specific Policies

The council also operates an 'Information Security Incident Reporting' Policy to comply with the requirements of the GDPR to manage information security incidents (data breaches).

Who does this policy apply to?

The Information Governance Strategy and corresponding policies apply to all council officers, any authorised agents working on behalf of the council, including temporary or agency staff, elected members, and third party contractors. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

What does this policy apply to?

The Information Governance Strategy and corresponding policies apply to information in all forms including, but not limited to:

- hard copy or documents printed or written on paper
- information or data stored electronically, including scanned images
- communications sent by post/courier or using electronic means such as email, fax or electronic file transfer
- information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card
- information stored on portable computing devices including mobile phones, tablets, cameras and laptops
- speech, voice recordings and verbal communications, including voicemail
- published web content, for example intranet and internet
- photographs and other digital images.

Strategic objectives

The strategy aims to develop a robust information governance framework with the following features:

- There is effective oversight of information management matters at the top level of the organisation.
- The information governance policy suite is effective and accessible to all employees.
- The roles and responsibilities of the SIRO and Veritau (the council's information governance advisors) are well established and widely known.
- A register of information assets has been compiled and information asset owners identified to ensure assets can be effectively managed and risks identified.
- Systems and processes are in place to securely store, transmit and dispose of information (both electronic and manual records).
- ICT Services implement technical solutions and procedures to protect personal data and minimise any potential security risks, including unauthorised disclosure of information, and seek national accreditation where appropriate.
- A layered framework of mandatory information governance training ensures employees receive information governance training commensurate with their role.
- A data protection officer has been appointed to support and direct compliance with GDPR.
- Systems have been implemented to enable information security incidents to be reported and investigated.
- Information security incidents are used to identify patterns and areas for improvement.
- Regular compliance checks are undertaken by internal audit, with the results used to shape future improvements.
- Key information risks are recognised on a specific information governance risk register and incorporated into the corporate risk register.
- Data Protection Impact Assessments are used to identify and address privacy risks associated with 'high risk' information processing, such as profiling.
- Personal information is collected and used responsibly, securely and fairly.
- Privacy notices are transparent and concise.
- Data subject rights are at the centre of service provision and understood by all employees.
- The council is signed up to the Multi-Agency Information Sharing Protocol and information sharing with delivery partners has been formalised through written agreements under the protocol and subject to appropriate monitoring.
- Data processing arrangements are documented in a contract, which includes data processing clauses. and such arrangements are subject to appropriate monitoring.
- Any use of cloud computing technology is compliant with legislation.
- Consider the value of signing up to codes of conduct and certification mechanisms as these become available.

These strategic objectives are regarded as fluid and subject to change and development as the council reacts to business change, emerging information governance risks and as national guidance on the GDPR and DPA emerges.

The council's DPO will submit an information governance plan to the council's senior management and the Audit, Governance and Standards Committee annually - this plan will include the council's annual information governance strategic objectives.

Information risks

One of the objectives of the council's Information Governance Strategy is to ensure the confidentiality, integrity and availability of information held by the council by reducing the risk of:

- unauthorised access to data
- incomplete or inaccurate data
- the unnecessary use of data.

Information risk management is the process of analysing, evaluating, assessing and mitigating the impact of risks to an organisation's information and information systems. Information risks must be managed effectively, collectively and proportionately, to achieve a secure and confident working environment.

Risks can never be eliminated fully. A structured, systematic and focused approach to managing risk is therefore required. However risk management is not about being 'risk averse', it is about being 'risk aware'. Some degree of risk taking is inevitable and necessary if the council is to achieve its objectives. By being 'risk aware', the council is in a better position to avoid threats, take advantage of opportunities and ensure its objectives and goals are realised.

Roles and responsibilities

In order to ensure that transparency, data protection, and other core information governance principles are embedded within the council's ethos and culture the council should appoint individuals to be responsible for information governance and data protection matters.

The council maintains the following information governance roles:

- Senior Information Risk Owner (SIRO)
  The SIRO is responsible for the council's overall information governance strategy and will be responsible for appointing the Data Protection Officer, the Specific Point of Contact(s), and the Information Asset Owners.

  The SIRO is accountable for the council's compliance with information governance legislation.

- **Data Protection Officer (DPO)**
  The DPO is a statutory position (Articles 37-39 of the GDPR) and:
  - Is the point of contact for the Information Commissioner's Office (ICO) and data subjects
  - Will facilitate a periodic review of the corporate information asset register and information governance policies
  - Assist with the reporting and investigation of information security breaches
  - Will provide advice on all aspects of data protection as required, in particular Data Protection Impact Assessments and Information Sharing Agreements.
- **Specific Point of Contact (SPOC)**
  The SPOC is responsible for overseeing the council's day to day information governance practices and in particular facilitate the process for reporting information security breaches to the ICO.

  The SPOC will work with the DPO and SIRO to ensure that corporate policies, processes, and decisions are implemented throughout the organisation.

The current contact details for these officers are:

Senior Information Risk Owner (SIRO)
Dr Justin Ives
Chief Executive
Justin.Ives@hambleton.gov.uk

Specific Point of Contact (SPOC)
Gary Nelson
Director of Law and Governance (Monitoring Officer)
Gary.Nelson@hambleton.gov.uk

Helen Kemp
Director of Economy and Planning
Helen.Kemp@hambleton.gov.uk

Data Protection Officer (DPO)
Information Governance Team
Veritau Limited
infogov.HambletonDC@:veritau.co.uk

The council's information governance work will continue to be supported by specialist external advice from Veritau Limited, who is also the council's DPO.

The council will also appoint Information Asset Owners to assist the SIRO in implementing the information governance framework - this is set out in the council's Information Management Policy.

Corporate Information Governance Group (CIGG)

A CIGG is a strategic group focused on setting high level strategic objectives, shaping the policy framework, determining the acceptable level of information risk and monitoring the overall adequacy of the information governance arrangements.

The council operates two CIGGs:

- Operational CIGG
  This group is made up of the SIRO, SPOCs, and representatives of the DPO to discuss the latest information requests (Freedom of Information, Environmental Information, and Data Protection requests) and to ensure the council responds to these requests in compliance with the relevant legislation. The DPO will provide the SIRO and SPOC with periodic request statistics prior to this meeting. This group meets monthly.
- Strategic CIGG
  This group is made up of the SPOCs and representatives of the DPO to discuss to set and track the council's strategic objectives. Other officers in the council will be invited to this group where required. This group meets quarterly.

Policy publication and review

The Information Governance Strategy and corresponding policies will be published on the council's website and will also be available to council officers and members via. the internal intranet.

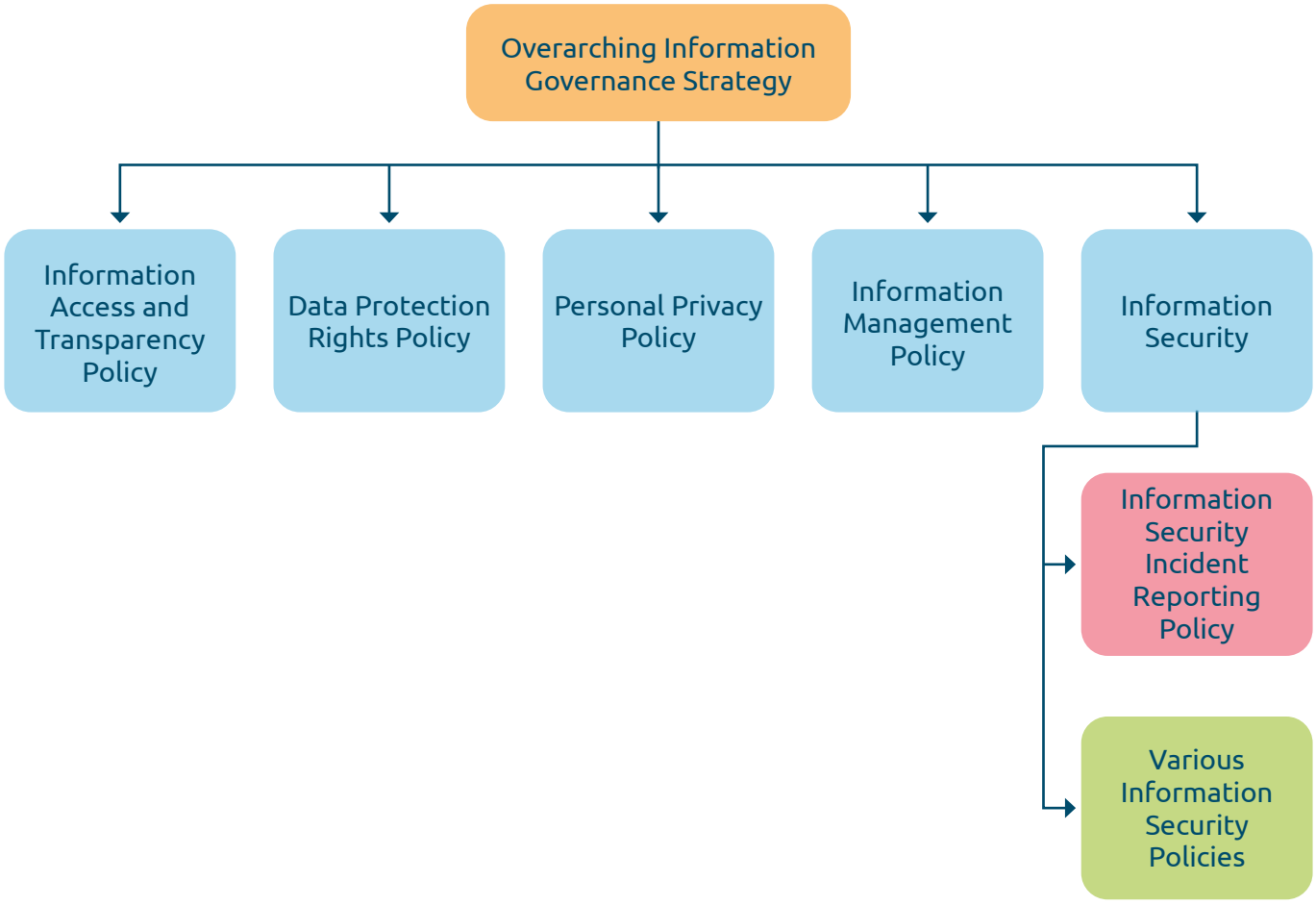
The strategy and policies will be reviewed annually by the DPO. Any significant changes to the policy suite will need to be approved by the SIRO who has devolved responsibility from elected members to do so.

Key messages

1. The council's Information Governance Strategy will seek to develop a robust information governance framework which is compliant with the requirements of the General Data Protection Regulation and Data Protection Act 2018
2. The council will be 'risk aware', rather than 'risk averse' in respect of information risks
3. Key roles of Senior Information Governance Officer, Data Protection Officer, Specific Point of Contact and Information Asset Owners will support the delivery of council's information strategy and will maintain periodic corporate information governance groups.

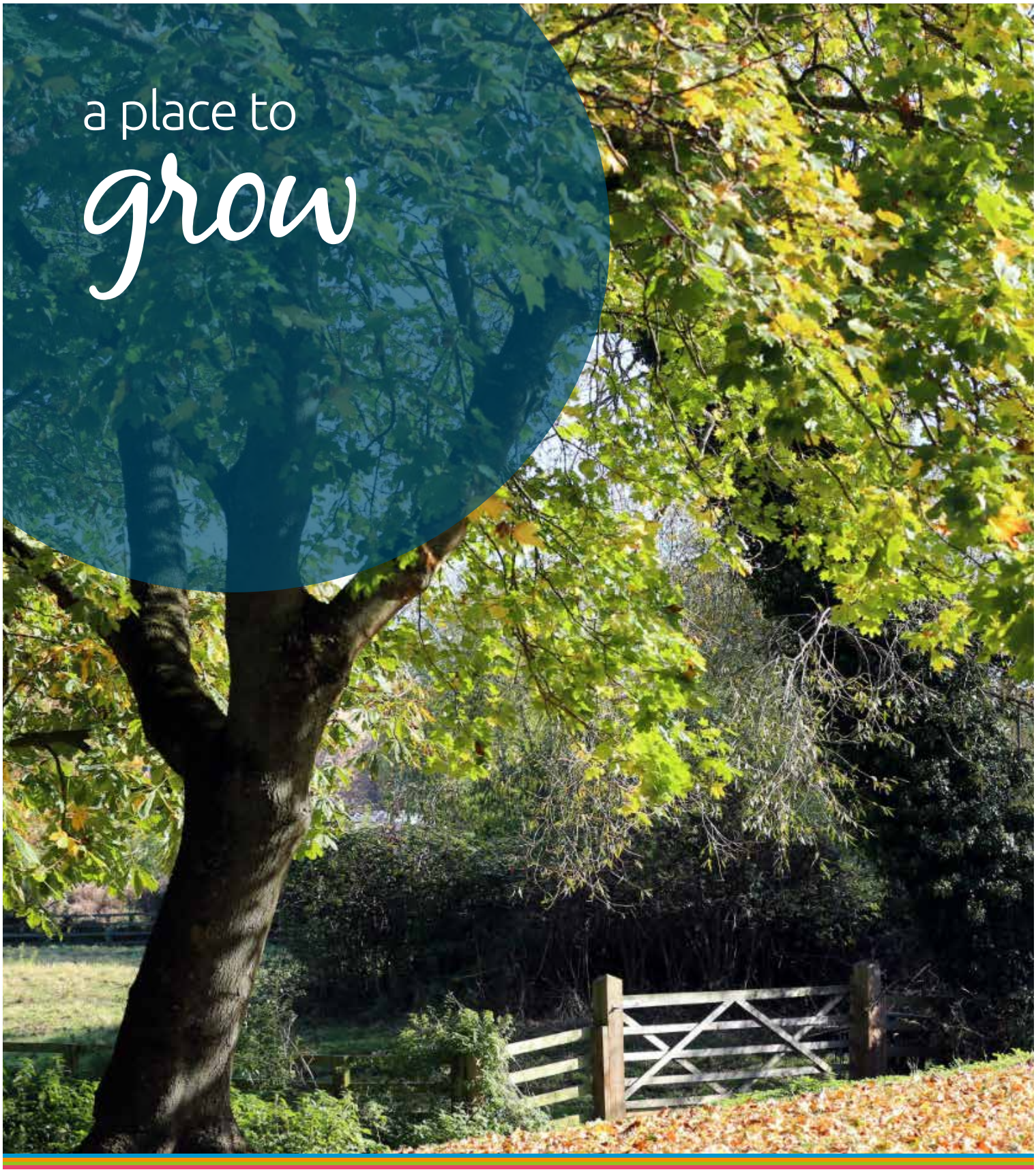
Appendix 1

Information Governance Policy Framework




HAMBLETON
STRICT COUNCIL


a place to
grow



HAMBLETON
DISTRICT COUNCIL

Civic Centre, Stone Cross, Rotary Way, Northallerton, North Yorkshire DL6 2UU
01609 779977
hambleton.gov.uk

This information is available in alternative formats and languages