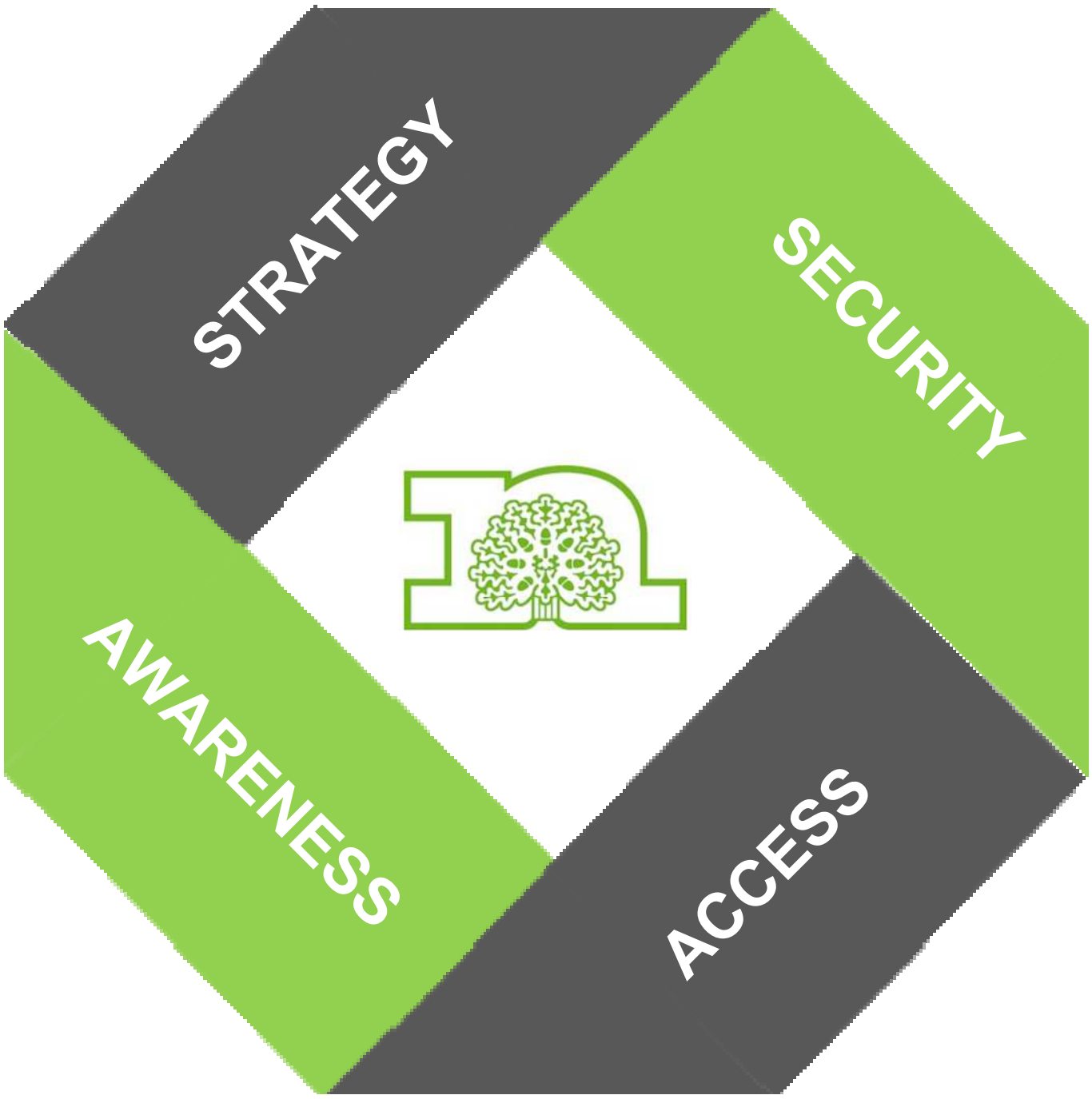
Appendix

INFORMATION GOVERNANCE IMPROVEMENT PLAN 2017



Programme Benefits

Better business performance

- Consistent and effective management of information across the Council.
- Increased understanding of, and compliance with, relevant legislation.
- Reduced number of information security breaches.
- Reduced actions and complaints against the Council as a result of poor information management, saving staff time and effort.
- Ability to improve data quality and analytics
- Clear responsibilities in relation to information governance and assurance.
- More streamlined, organised and efficient information retrieval
- Reduced information storage requirements
- Better business continuity provisions

Better collaboration and information sharing

- Improved information sharing statutory compliance.
- Improved protection of children and vulnerable adults.
- Increased ability to share information with partner agencies.

Increased public confidence

- Improved customer satisfaction due to faster access.
- Increased confidence in the management of personal information.
- Reduced risk to Council reputation.

Better risk mitigation

- Proactive compliance with regulatory and legislative requirements
- Improved information security and protection of data assets
- Effective management of information risks and ability to learn lessons
- Greater confidence that information risks are effectively managed across the Council's transformation and change programmes.

INFORMATION GOVERNANCE IMPROVEMENT PLAN

- Information Governance defined
- Information Governance roles and responsibilities defined
- Refreshed and streamlined policies

- User permissions reviewed and rationalised
- Information Sharing arrangements reviewed and systemised
- Information Governance designed into project initiation process
- Information breach process strengthened

STRATEGY

SECURITY

AWARENESS

ACCESS

OUTCOMES

- Mandatory Information Governance training re-designed
- Comprehensive communications plan developed
- User-friendly management reporting on Information Governance developed

- Clear and consistent, mandatory system for storing & managing information
- Controlled and compliant information retention
- Systems for the retention of archived information developed.

Information Governance Improvement Plan: Strategy - Actions

The challenges

- A lack of understanding of the value and importance of data and information (paper & electronic)
- Data breaches leave the Council vulnerable to a loss of public trust and confidence as well as significant fines.
- Poor document management practices.
- Lack of communicated commitment at a senior level results in a lack of managerial buy-in to improvement initiatives such as ensuring all staff are trained promptly, and the Information Asset Register being completed and maintained.

Define Information Governance and IG structures roles and responsibilities

[Sept 17 – Mar 18]

- Define strategic approach and definition of Information Governance
- Formalise IG work in Job Descriptions - IG team and other roles; (Senior Information Risk Officer (SIRO), Caldicott Guardian, etc).
- Communicate IG framework and roles
- Revise all roles and responsibilities alongside a re-structure of the information governance function

Refresh and streamline policies

[Sept 17 – Mar 18]

- Identify all existing policies and procedures
- Information Management Group (IM Group) to recommend for approval
- Suite of policies underpinned by guidance to Policy Committee for approval.
- Communication strategy and Information "hub" on the intranet.

Information Governance Improvement Plan: Security - Actions

The challenges

- Incomplete compliance with the requirements of current and forthcoming legislation (Data Protection Act 1998 and General Data Protection Regulation 2018) e.g. with regard to the retention and destruction of records.
- Risks of significant fines (£8m – 18m) for breaches and associated reputational damage
- Any failure to be legally compliant places service users' sensitive personal data at risk and leaves the Council exposed to claims of inadequate governance arrangements.

Review and rationalise user permissions

[Mar 18 – Aug 19]

- Map current user permissions (which govern individuals' access to data) against legitimate business use and location of records
- Agree role based permissions with relevant managers
- Agree principles for removal of "historic "permissions of current and former staff via IM Group
- Implement agreed permissions and remove historic permissions

Information Sharing

[Jan 18 – Dec 18]

- Review all existing data sharing agreements and identify gaps by cross referencing to Information Asset Register
- Refresh Council's Privacy notices on the website and consider future requirements.
- Devise and implement the use and recording of informed consent from service users when collecting their data together with ability to activate withdrawal of consent where appropriate
- Update Information Asset Register and develop protocols for ongoing maintenance & monitoring
- Review and implement security classifications and markings policy for documents and emails.
- Procure long term email/file transfer system with necessary budget provision.

Ensure risk assessment Process embedded in all new projects

[Sept 17 – Sept 18]

- Embed risk assessment and Privacy Impact Assessment (PIA) process at start of all ICT projects
- Ensure data protection controls and requirements are considered at the design stage of all new projects/initiatives
- Ensure data protection issues/questions included in all tender documents and suitable terms and data sharing/processing arrangements are included in all contracts let.

Strengthen breach monitoring process

[Oct 17 – May 18]

- Revise breach categories to align with ICO definitions
- Devise risk rating system for better management, monitoring and reporting of breaches
- Use risk rated reports for 6 monthly performance reporting to Committee and Leadership teams.
- Provide enhanced IG support to Departments for data breach investigations
- Improve analysis of incidents and capture/implementation of lessons learned

Information Governance Improvement Plan: Awareness - Actions

The challenges

- The current “one size fits all” basic approach to training is not resulting in tangible improvements in Information Governance practice
- Continuing information breaches (4 self-reported incidents to the ICO in the past year).
- Cultural change in the way information is dealt with and managed has not occurred to the degree required to minimise the significant risk to the Council.
- Lack of systems to easily identify when training has taken place and enable managers to monitor compliance.

Create mandatory bespoke NCC training

[Sept 17 – Mar 19]

- Mandatory induction training - entry level training for all within 4 weeks of starting
- Role based training will be developed for all practitioners - eg social care, legal - in high risk areas
- Refresher training will be required at 2 yearly intervals
- Specific face to face team based training will be developed for those without PC access
- Training for specific posts eg SIRO, Caldicott Guardian, Data Protection Officer etc
- All training will be reviewed every 2 years to ensure it reflects current best practice & legal requirements

Communication and culture change

[July 17 – Aug 19]

- Devise and implement 2 year communication strategy in relation to all areas of this plan.
- Direct work with Group and Team Managers, Leadership and training meetings, Directors Business meetings and with teams identified as high risk.
- Regular reporting to Corporate Leadership Team (CLT), on data breaches and plan implementation
- Regular reporting to Governance & Ethics Committee on data breaches, implementation of this plan and areas for improvement

Enable timely more user friendly management reporting

[Sept 19 – Aug 19]

- Include in the Business Reporting / Management Information project a workstream to extract information from the Learning Pool to report to managers.

Information Governance Improvement Plan: Access - Actions

The challenges

- A lack of understanding of the value and importance of data and information (paper & electronic)
- Inconsistent information storage.
- Inconsistent and limited approach to information archiving
- Lack of clear file structures or corporate identity.
- File access arrangements lack sufficient control.
- Multiple copies of files often lacking ownership.
- Risks of only limited compliance with information governance legislation

Create clear consistent mandatory system for storing and managing information

[Mar 18 – Aug 19]

- Review current structure to determine common areas, functions and any unique requirements
- Develop file plan principles - approved by CLT
- Create cross council file plan in line with approved principles - agreed with Departments
- Create structure within networked directories & effect transfer of information
- Pilot process in some identified areas of the Council - then roll out
- Identify historic data without a data owner and transfer into file plan
- Removal of H drives - current business related information to be moved into corporate file structure, historic information to be archived and retained (IICSA)
- Understanding of and adherence to principles included in job competencies

Ensure data retained in accordance with law

[Sept 17 – Dec 17]

- Update retention schedules (initially with guidance from Records Management Service)
- Include exemption from destruction protocols for any records pertinent to IICSA
- Align Information Asset Register entries to ensure consistency with retention schedules
- Communicate new requirements and devise online training module.

Develop approved systems for retention of archived data

[Sept 17 – Aug 19]

- Identify all current means and location of data storage (paper and electronic)
- Establish project to consider options to streamline information storage in future (including cost/benefits)
- Options appraisal to be drawn up for consideration by CLT