



Derby City Council

COUNCIL CABINET **15 April 2015**

ITEM 16

Report of the Cabinet Member for Governance and Transformation

Document Classification Scheme

SUMMARY

- 1.1 In April 2014, central government's Cabinet Office introduced a revised document classification scheme that is applicable across all public sector organisations, including local authorities. It applies to all information that is collected, stored, processed, generated or shared to deliver services and conduct business, including information received from or exchanged with external partners, including arms-length management organisations of public bodies.
- 1.2 In practical terms, the scheme obliges all information in and out of the Council to be classified so as to provide a means of identifying the level of sensitivity of the detail they contain. The scheme goes further than merely impacting on documentation however, as the Cabinet Office guidance makes it clear that ICT systems and services may require enhanced controls to manage the associated risks to aggregated data or to manage integrity and availability concerns.
- 1.3 There are four key principles underpinning the scheme, namely that:
 - (i) all information has intrinsic value and so require an appropriate degree of protection;
 - (ii) everyone who works with a public organisation, including contractors and other service providers do so under a duty of confidentiality, creating a responsibility to safeguard data they access, whether or not it is expressly marked, and must be provided with appropriate training;
 - (iii) access to sensitive information must only be granted on the basis of a genuine 'need to know' and with appropriate personnel security controls in place;
 - (iv) assets received from or exchanged with external partners must be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations
- 1.4 All public bodies are expected to apply the scheme. All staff and elected members will therefore be subject to it. Public bodies are also required to ensure that a consistent scheme is applied and operated by their delivery partners, such as Derby Homes Ltd., and their wider supply chains.

RECOMMENDATION

- 2.1 To approve the Council's document classification scheme set out in Appendix 2 for introduction and implementation across the Council.
- 2.2 To authorise a change to the Council's Contract Procedure Rules to ensure that it incorporates a requirement that all contractual partners are obliged to apply the Council's scheme in the delivery of any contracted services undertaken on the Council's behalf, and to receive training on it.
- 2.3 To authorise the Strategic Director for Adults, Health and Housing to ensure that arrangements are put in place for Derby Homes Ltd. to adopt and apply the Council's scheme, including its training requirement.
- 2.4 To note the implementation of the TITUS electronic document classification project to give effect to the operation of the Council's scheme.
- 2.5 To note that mandatory training using the e-learning portal will be rolled out across the organisation, for all staff and members.

REASONS FOR RECOMMENDATION

- 3.1 To enable the Council to implement the Cabinet Office obligation to secure the implementation of the Government Security Classifications Guidance (April 2014).

SUPPORTING INFORMATION

- 4.1 The scheme identifies three security classification groups – Official, Secret and Top Secret.
- 4.2 The Official classification works on the premise that all information into and out of a public body is official information that affects the day-to-day business of the organisation, no matter how routine the nature of the information is. So far as the Council is concerned, it is anticipated that practically all of the correspondence, information and other data it receives or sends will fall into this classification category.
- 4.3 The Secret classification is defined in the guidance as *‘very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime’*.
- 4.4 The Top Secret classification is defined in the guidance as *‘HMGs most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations’*.
- 4.5 The Council’s scheme does not make provision for either of the classifications detailed in paragraphs 4.3 or 4.4 as it is considered highly unlikely that local authorities will have to process such information using their routine business systems. In the very rare event that either extreme circumstance is triggered by government, requiring a response from the Council, it is clear that relevant information will be handled on a person-to-person basis.
- 4.6 The Council’s scheme therefore focusses on the Official classification only. Although the guidance does not expressly require all documentation to be identifiably marked, officers consider that in the interest of consistency across the Council, all documentation should in fact be marked. Doing so assists with implementing a culture change that safeguards the Council’s position in so far as it requires each document author to have regard to the scheme principles in every case.

- 4.7 To complement this culture change, officers have been working to introduce the TITUS Document Classification project. TITUS is a piece of software we will deploy to every user, computer and mobile devices. It allows you to flag documents, spread sheets, Power Point files, emails and Adobe documents with the appropriate protected marking. TITUS does not apply a default marking to documents but rather provides a command prompt, which cannot be overridden, that requires a document author to apply a classification to whatever document is being produced. It will apply to every document created electronically including routine letters; Microsoft Office based documentation as well as email.
- 4.8 The Official classification that will apply to the Council's scheme, in line with the Cabinet Office guidance, has a further sub-split between routine official documentation and official documentation that is statutorily classed as 'sensitive', as defined within the Data Protection Act 1998. While consideration was given to further sub-splits, in the interest of maintaining simplicity and consistency across the range of Council services, officers do not consider that there is a need to go further than these two sub-set categories as that would create unnecessary complexity with the potential to give rise to inconsistency and confusion.
- 4.9 In its simplest form therefore, all routine documentation including those that contain personal information will be classed as 'Official', with only those falling within the statutory definition of personal sensitive data contained in section 2 of the Data Protection Act 1998 being classed as 'Official – Sensitive', namely information relating to a person's:
- A. racial or ethnic origin;
 - B. political opinions;
 - C. religious beliefs or other beliefs of a similar nature;
 - D. membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
 - E. physical or mental health or condition;
 - F. sexual life;
 - G. commission or alleged commission of any offence; or
 - H. Involvement in any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.
- 4.10 It is acknowledged, and permitted within corporate rules, that ad hoc personal mail or other correspondence which is not work related does sometimes arrive for staff. Similarly, discreet use of email for limited personal use by staff is permitted. Both as a reminder to staff therefore as well as to the recipient of such documentation, TITUS will offer a third classification category identifying that such exchanges are personal to the parties to it and that as such the information contained within it should not be regarded as council authorised information.

- 4.11 We will need to include as a mandatory requirement in future tenders, including those for new IT systems, the need for the supplier to manage data in accordance with these security classifications and to include features that can add a security classification when producing reports or aggregating data; this will need to apply to both live and archived data.
- 4.12 It is important to emphasize that it is the nature of the data that determines the classification and it is not who it is being sent to or received from; there is a common misconception that because the data is being sent within the council, there is no need for it to be classified; that is incorrect.
- 4.13 Details of the proposed scheme are set out in Appendix 2, while at Appendix 3 is the Cabinet Office document 'Government Security Classifications (April 2014)'. Appendix 2 also incorporates a worked matrix to assist users with assessing the appropriate marking to be applied.

OTHER OPTIONS CONSIDERED

- 5.1 None.

This report has been approved by the following officers:

Legal officer Financial officer Human Resources officer Service Director(s) Other(s)	Janie Berry Toni Nash Liz Moore
---	---------------------------------------

For more information contact: Background papers: List of appendices:	Olu Idowu 01332 643615 e-mail olu.idowu@derby.gov.uk None Appendix 1 – Implications Appendix 2 – Protective Marking Scheme draft categories Appendix 3 – Government Security Classifications April 2014 - PDF
---	---

IMPLICATIONS

Financial and Value for Money

- 1.1 The TITUS document classification software has previously been budgeted for within ICT. There is no additional cost to the Council arising from its implementation.
- 1.2 Similarly, other than the staff time required to draw up and upload the training program to the e-learning portal, there are also no additional costs to the Council arising from its implementation.

Legal

- 2.1 The report sets out the legal basis for implementation of the scheme.

Personnel

- 3.1 All staff and members will need to be trained in the use of the new classification system, and this will be rolled out through the Council's e-learning portal.

IT

- 4.1 Implementing the TITUS system will allow us to add official marking to emails and to documents created in word and Excel, this will go some way to meeting the requirement but requires staff to use the prompts and add the markings. There is an alternative for Word but again it would require users to adopt it, we could create two word templates with footers pre-defined as Official and Official Sensitive. The Titus system is however a better solution. Note the letter head templates will not need changing but will need to be applied in combination with the Titus system to allow for the correct classification to be added to the footer.
- 4.2 The TITUS system does not cover all Information systems, many of which have both standard reports and the ability to produce ad-hoc reports. Instead we will need the authors of such reports to generate a protective marking classification; it will take some time to achieve this and the recommendation is that reports are amended the next time they are generated. This will require expert users, system administrators and Information Systems staff to make the necessary changes.
- 4.3 The corporate EDRMS has an existing data classification scheme which will now be amended, this requires the person loading the documents to the EDRMS to add a classification, we will set a default of official and users will have to amend this to official sensitive where that is the correct classification.

- 4.4 Adopting the rules in this report for deciding if data is official or official sensitive will also need to be applied to the information asset registers such as the systems and databases are also given the same classification. This would mean systems like HR Payroll, Youth Offending and social care (both Adults and Children) should be classified as systems containing official sensitive data (even if not all data they contain is such).

Most systems would be classified as official but the information asset owner needs to decide for each system, for example some systems may include data about health or disability which would trigger the higher official sensitive classification. Using the examples to classify the systems is important because we need to consider if any additional data access or data storage controls are required; for example the use of two factor authentication for remote user access.

Equalities Impact

- 5.1 This system will further protect the sensitive information about disabled people, minority ethnic people, LGBT people and people's religion or belief.

Health and Safety

- 6.1 No Implications

Environmental Sustainability

- 7.1 No Implications

Property and Asset Management

- 8.1 Other than in relation to the detailed IT implications in paragraph 4, there are no other asset management implications.

Risk Management

- 9.1 If the Council does not adopt this or another similar classification scheme, then any data handling breaches, that could have been averted if such a scheme was in place, could result in the Council being subject to sanctions from the ICO.

Corporate objectives and priorities for change

- 10.1

OFFICIAL

Definition:

The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.

Examples:

- press releases
- public registers (including electoral register) annual reports/accounts
- Corporate policies and procedures
- business plans
- information on www.derby.gov.uk
- historical records
- internal reports, memos and emails
- minutes of meetings
- equality impact assessments
- Debtor records
- Records relating to benefits paid
- Passports
- Birth certificates
- routine correspondence
- City plans

OFFICIAL SENSITIVE

A limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost stolen or published in the media. This subset of information should still be managed within the 'OFFICIAL' classification tier, but should attract additional measures (generally procedural or personnel) to reinforce the 'need to know'. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know' assets should be conspicuously marked: OFFICIAL SENSITIVE.

Information to be designated within this category are those falling within the statutory definition of sensitive personal data as defined in section 2 of the Data Protection Act 1998 concerning information about a person's:

- a) racial or ethnic origin
- b) political opinions,
- c) religious beliefs or other beliefs of a similar nature,
- d) membership of a trade union (within the meaning of the M1Trade Union and Labour Relations (Consolidation) Act 1992),
- e) physical or mental health or condition,
- f) sexual life,
- g) commission or alleged commission of any offence, or
- h) proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

Examples:

Individual records relating to:

- Sick notes
- Social care
- Special educational needs
- internal investigation reports
- Payroll information
- Health
- Visual impairment register entries
- Tenancy applications and agreements (subject to specific content)
- Personnel records (subject to specific content)
- Schools Pupil data

- Risks to Children lists
- Adoption files and registers (including those of the adopter)
- Completed ballot papers
- Foster carer files (including those fostered)
- Information on vulnerable people or minors
- Benefit investigation files
- National pupil database
- Looked after children data and files
- Disclosure & Barring Service (DBS) (formerly CRB) records

Examples also include bulk entries likely to include some or all of any of the examples listed above. Typically this would apply to databases of information held.

** Examples given for both 'Official' and 'Official Sensitive' are not exhaustive!*

PERSONAL

Although not a requirement of the Government Classification Scheme, a third category of classification will be permitted by the Council under this heading, acknowledging that staff are permitted limited but responsible use of email for personal purposes. For the avoidance of doubt, such use is subject to compliance in all respects with the Council's 'Email and Internet User Policy' (link below).

<https://iderby.derby.gov.uk/it/it-policies-and-procedures/email-and-internet-policy/>

Type of Document	Justification Criteria								Remarks
	Racial or Ethnic Origin	Political Opinions	Religious Beliefs	TU Membership	Health	Sexual life	Commission of alleged commission of Offence.	Proceedings for any Offence.	
Sick Notes					X				
Accident Books					X				
Social Care Records					X	X	X	X	
SEN					X				
Internal investigation reports	X		X	X	X	X	X	X	
Payroll information				X					

Type of Document	Justification Criteria								Remarks
	Racial or Ethnic Origin	Political Opinions	Religious Beliefs	TU Membership	Health	Sexual life	Commission of alleged commission of Offence.	Proceedings for any Offence.	
Health					X	X			
Visual impairment register entries					X				
Tenancy applications and agreements subject to specific content)	X							X	
Personnel records	X		X	X	X	X		X	
Schools Pupil data	X		X		X	X			
Risk to Children list					X	X			

Type of Document	Justification Criteria								Remarks
	Racial or Ethnic Origin	Political Opinions	Religious Beliefs	TU Membership	Health	Sexual life	Commission of alleged commission of Offence.	Proceedings for any Offence.	
Adoption files and registers (including those of the adopter)	X		X		X	X			
Completed ballot papers		X							
Foster carer files (including those fostered)	X		X		X	X			
Information on vulnerable people or minors	X		X		X	X			
Benefit investigation files							X	X	
National pupil database	X		X		X	X			

Type of Document	Justification Criteria								Remarks
	Racial or Ethnic Origin	Political Opinions	Religious Beliefs	TU Membership	Health	Sexual life	Commission of alleged commission of Offence.	Proceedings for any Offence.	
Looked after children data and files	X		X		X	X			
DBS (formerly CRB) records								X	

