Mandate Information Governance Relevance Check

This tool will identify the Information Governance (IG) impacts of a new change proposal. Complete part 1 of this form and it along with the project mandate, if you have one, to Information.management@bristol.gov.uk so that the Information Governance Service can provide professional advice and guidance.

Part 1: project / change proposal details

What is the proposal?	
Name of proposal.	
Please outline the proposal.	
Who will answer any queries regarding the responses provided on this form?	

Does the change/project involve processing personally identifiable or special category information?
Please outline what Personal or Special Category data will be processed (see definitions below)?
Acquisition, processing, storage or disposal

Will the change/project involve other organisations? Is this likely to involve exchanging information with them?
Please outline which type of organisations e.g. internal BCC departments, voluntary sector, NHS etc. might receive our data and information as part of this project or to support the changes it proposes.
internal BCC departments, voluntary sector

Is the change/project likely to provide/create or require new information? Or information analysis to support performance management, planning or decision making?
Please outline any new data or information the project/change will create.
none

Will the change/project produce any publishable Open Data? (non-personal and non-commercially sensitive data)
Please see http://intranet.bcc.lan/ccm/content/articles/transformation/information-management-prog/information-we-publish.en and detail what data might be 'Open' below
[Enter your response here]

Is the change/project likely to change the acquisition, processing, storage or disposal of information?
Please outline the changes the project is likely to make (see definitions below)?
no

Have you considered what security measures need to be in place?

Please outline the security testing which will be needed e.g. the ability to audit third party suppliers and their systems, penetration testing.
none required for the Full Business Case

Approvals	
Person completing the Information Governance Relevance Check (e.g. project manager, manager)	
Person owning the change project / proposal (e.g. Service Manager, Director)	

Part 2: comments from Information Governance Service

Advice and guidance	
Data Protection Officer	
Information Security Manager	
Records Manager	
Information Management Advisor	
Freedom of Information Officer	
Head of Information Governance / Statutory Data Protection Officer	

If you are working on a formal business case (mandate, outline or full business case) then the comments above should be incorporated into the 'professional views' section of the business case.

Definitions

Acquisition, processing, storage or disposal	'Acquisition' includes the collecting, buying, generating and obtaining from other bodies; 'Processing' includes the disclosing, viewing, amending, transmission, and combining; 'Storage' including archiving (in any format including paper), hosting, cloud storage; and 'Disposal' includes the retention, deletion, destroying or not disposing of information.
Personal Data	any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Special Categories	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Penetration testing	The practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit