Appendix A

Information Governance Improvement Programme: Key Developments (as at May 2018)

Please note: data processing means anything which is done with data (e.g. collection; sharing; storing; sending; destroying etc).

What GDPR requires	What has been done	Next steps
GOVERNANCE		
An effective **governance regime** which ensures roles and responsibilities are clear; timely decisions are made and the information governance regime across the Council is monitored and reviewed	Key roles / decision-makers defined in the new Information Governance Framework. New and revised information governance role descriptors in place (e.g. for Information Asset Owners; System Owners etc). Key Performance Indicators developed and reporting arrangements established (routinely through Information Governance Group at a corporate level and Risk Safety and Emergency Management Groups at a departmental level). Visibility through regular reporting to Governance and Ethics (G&E) Committee.	Regularised and on-going performance and risk reporting to agreed governance bodies to enable the whole system approach to be monitored.
Policies, procedures and standards which reflect the new law and good practice and detail how this will be implemented within the Council	New Information Governance Framework and supporting information compliance, rights and security policies approved by Policy Committee (March 18) New priority procedures approved including CCTV/surveillance; Data Protection Impact Assessments; Information Sharing; Consent etc.	Remaining, lower priority procedures and standards to be drafted and approved by Information Governance Group (IGG) finishing by Sept 2018. Review the need for an Appropriate Policy Document (to augment data protection policies in respect of the processing of special category data) as

	Information security standards approved including patching, passwords, encryption etc. Revised information security standards approved by IGG – encryption; patching; passwords etc;	per the provisions of the Data Protection Act (2018). Policy, standards and procedures suite to be kept under regular (annual) review and updated in accordance with Information Commissioner's Office (ICO) and other guidance, good practice, enforcement, case law etc.
Ensure that the Council can respond to mandatory **data breach reporting** to the ICO within 72 hours and that technical and organisational improvements are made as a result of breaches	Revised IT Major Incident Procedure and corporate Data Breach procedure in place. Scenario testing by corporate Risk, Safety and Emergency Management Group (RSEMG) of major incident – power outage (March 2018)	Continue to monitor breaches and link their root causes to targeted remediation plans and communications so that systemic improvements are made.
AWARENESS & TRAINING		
Ensure there is **awareness of GDPR** across the organisation and raise the profile of data protection	Programme Communications Plan in place. Resources library established for staff to access. Numerous meetings attended to showcase and raise awareness of the requirements of GDPR across and at all levels of the organisation. Numerous articles written for Team Talk etc. Chief Executive's Blog has focussed on the new data protection law and the associated programme a few times, demonstrating commitment from the top.	Full revision of Intranet and Internet information governance pages and resources (Autumn 2018)

An information governance/data protection **training** programme for all staff, with top up, role specific training for staff with a particular requirement for a more detailed understanding (e.g. social care staff; project managers; commissioners; contract managers etc)	Researched, secured and rolled-out new GDPR compliant, local government specific e-learning. Mandatory for all PC using staff to complete, 3919 (of 4898 – 80%) have completed (at 16 May 2018) Elected Members given access to elearning. Developed and rolled out paper-based training for staff who do not use personal computers. Mandatory for all non-PC using staff to complete, 2093 (of 3214 – 65%) have completed (at 16 May 2018) Training information for asset managers (i.e. group/service/team managers) rolled out as part of the information asset register exercise (see below). Developed and agreed training standards for all roles with a specific information governance dimension	Design of role specific training completed and rolled out (June to October 2018). Elected Members training sessions as top-up to elearning, as set out in report to Full Council (May 2018).
RESOURCES		
Appoint **Data Protection Office**r to assure data protection compliance within the Council and to be the point of contact with the ICO. It is mandatory for the Public Bodies to have a suitably trained DPO	Unable to recruit to DPO in buoyant market. Contingency measures implemented and DPO in place. DPO contact details established, referenced in privacy notice and notified to ICO.	

Ensure an **adequate level of resource** to maintain performance on an on-going basis.	Business case for additional resources considered and agreed by Corporate Leadership Team (CLT); G&E Committee and approved by Finance and Major Contracts Committee (Jan 2018) Recruitment underway for new staff to become business partners, supporting the information governance efforts of departments. Contingency measures in place to extend the duration of the initial phase of IGIP to cover business as usual support if there is a failure to recruit in the current labour market.	Review of resourcing arrangements due December 2019, with changes arising to take effect from April 2020.
DATA PROTECTION PRINCIPLES & RIGHTS		
Understand what personal information is held, why it is held and what is done with it by developing a record of processing activities, and keeping this under review	Redesigned the Information Asset Register (IAR) to be GDPR compliant. An IAR contains logical groupings of information so that information risks can be assessed. Undertaken pilot and follow-up Council-wide exercise to populate the new IAR. Number of recorded assets has gone from 586 (June 17) under the old register to 2,483 (May 18). Identified risks arising from the IAR and sent individual teams action plans to address those risks.	Monitor and report on the implementation of action plans. Put in place a method and plan to ensure that the IAR is a 'live' document of information assets held by the Council so that risks can continue to be identified. Research options for a better technical solution for maintaining the IAR, preferably an integrated system capable of managing a variety of aspects of information governance.

Put in place **Privacy Notices** to advise people about the collection and use of their data - what is held; why it is held; what is done with it; who it is shared with; how long it is kept for etc. In line with the data protection principle of transparency.	Researched guidance and good practice from elsewhere to establish an approach to NCC privacy notices (agreed Jan 18). Updated the corporate privacy notice to ensure that it is compliant with the Data Protection Act (1998) in November 2017. Updated the corporate privacy notice to ensure that it is compliant with the GDPR in May 2018. Updated a key service privacy notice (adoption service) as a template for future, service specific notices.	Put in place online, service specific privacy notices by early September 2018 and update business forms, where appropriate, in line with those notices.
Ensure systems and processes are in place to comply with other **data protection principles** including: - Limiting data processed to a minimum - Keeping it for only as long as necessary - Controlling its access - Maintaining its accuracy - Keeping it safe	Undertaken systems audit of NCC business critical systems. Need for Data Protection Impact Assessments (DPIAs) identified. Systems Level Security Management Procedure approved to ensure that there is a single register of all systems which process personal data within the organisation, with details of how they are used and their security standards. New Retention Schedule drafted, approved and informed IAR exercise. Initial scoping of business requirements needed from a document management system and preliminary research on good practice undertaken	Further diagnostic work to be undertaken on NCC standard and decommissioned systems, with resultant action plan in place to address gaps / risks. Develop and populate the Systems Level Security Register and address gaps / risks identified as a result. Business case for document management system completed (Sept 2018).

Embed **Privacy by Design and Data Protection Impact Assessments (DPIAs)** into the business to ensure privacy impacts of business change are minimised and there is a robust risk assessment of high risk personal data processing	New DPIA procedure, including register and metrics for monitoring, drafted and approved. DPIA procedure cross-referenced to other business change procedures (e.g. in project management documentation) Training workshops undertaken with key staff (e.g. project managers) List of DPIAs compiled, prioritised and assigned. There will be greater ability to complete DPIAs once staff team in place. Numbers of outstanding DPIAs (over 150) are challenging in terms of capacity to complete and associated risks.	Performance on DPIAs reported regularly to Information Governance Group and departmental Risk Safety and Emergency Management Groups. Procedure reviewed annually and amended for changes in good practice, case law etc.
Ensure systems and processes are in place to comply with new and enhanced **data subjects rights,** including: - responding to Subject Access Requests (SARs) - the right to be forgotten (i.e. data deleted / destroyed) - Higher bar for managing consent to process data	Revised SAR procedure approved. Consent procedure approved. The Council has duties and powers such that consent should only need to be used as a basis for processing data in exceptional circumstances.	Continue to monitor performance on SARs, with emphasis on response times against new, shorter GDPR requirement of one month (as opposed to 40 days). Examine requirements for procedures around other aspects of data subject rights (right to be forgotten etc.).
SUPPLIERS & THIRD PARTIES		

Ensure **suppliers are compliant with the GDPR** where processing personal data on the Council's behalf and that there is a contract and data processing agreement in place.	Risk assessed Council suppliers and informed them of intention to vary existing contracts in line with the government's recommended standard. Prioritised plan in place to undertake the contract variation programme. Established data processing requirements of suppliers to inform contract variations. Piloted new procurement criteria and due diligence questions to ensure future suppliers are able to meet GDPR requirements.	Continue to vary contracts with suppliers in line with plan. Monitor implementation of new procurement requirements, particularly in respect of any adverse impacts on supplier availability.
Provide **GDPR assurances to those organisations for whom the Council processes personal data** (e.g. schools)	Prepared a GDPR statement and provided guidance to enable responses to enquiries from third parties for whom the Council supplies services which involve the processing of personal data.	Put in place a variation to the contract(s) the Council has with schools to supply services which involve the processing of personal data (e.g. payroll services)
Support **Nottinghamshire schools** in their efforts to become GDPR compliant	Although schools are data controllers in their own right, the NCC Education Improvement Service collaborated with Essex CC to provide a GDPR framework and associated training to Nottinghamshire Schools on a subsidised basis. The DfE has recently released its own Data Protection Toolkit for schools.	Explore the possibility of collaborating with the elearning provider to adapt product for use by schools staff, governors etc.