NEWARK & SHERWOOD DISTRICT COUNCIL

Document Name: Data Protection Policy

Effective Date: 4th October 2016

Date for Review: 4th October 2018

Version Number: 3.1

Approved by: CMT

Responsible Business Manager: Jill Baker

Newark & Sherwood District Council

Data Protection Policy

Occtober 2016

1. **Background.**

To be able to provide its statutory and discretionary services Newark & Sherwood District Council, the Council, collects and uses information about individuals. This will include information on members of the public, customers, suppliers, employees (past and current) and all others with whom the Council communicates.

In handling personal information the Council is required, by law, to fulfil certain statutory duties and, in particular, to comply with the terms of the Data Protection Act 1998 (DPA) and also to work toward compliance with the General Data Protection Regulation (GDPR) adopted by the European Parliament on 14th April 2016 and coming into full effect in May 2018.

GDPR builds on current data protection legislation across member states to consolidate this into a common set of standards that will apply to the processing of personal data for any European citizen, wherever that citizen may reside or wherever the processing takes place. The requirements of GDPR, in general, set a higher level of responsibility upon individuals and organisations processing data than current legislation and will replace the DPA in May 2018.

Following the referendum held on 23rd June 2016 the Information Commissioner announced that from May 2018 GDPR will be the effective legislation as the United Kingdom will at that stage still be a European member state. However, Data Protection legislation in the United Kingdom will then have to be changed to align with many of the key requirements of GDPR once the UK ceases to be a European member state.

All Data Controllers have therefore been encouraged to develop their policies to anticipate the higher standards set by GDPR whilst recognising that the prevailing legislation is currently the Data Protection Act 1998.

This policy therefore incorporates many elements which the Information Commissioner currently recommends as good practice in line with GDPR but which will become mandatory as the legislative framework evolves.

The policy also recognises that the Council is changing many of its working practices and work styles and therefore contains specific sections on home and off site working, data sharing with partners and supplier and assessing risk to personal data.

2. **Scope of this Policy.**

This Policy applies to all employees and members of the Council. Any breach of the Data Protection Act 1998 or the Council's Data Protection Policy may be considered to be a breach of the Members' Code of Conduct or the staff disciplinary procedures. As a matter of good practice, other agencies and individuals working with the Council, who have access to personal information, will be expected to read and comply with this Policy.

3. **The Data Protection Act 1998.**

The Data Protection Act 1998 came into force on the 1 March 2000, and widens the scope of the Data Protection Act 1984. Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent.

3.1. Definitions

3.1.1. **Personal data** - means data in any format which relates to a living individual who can be identified from those data or from those data and other information which is in the possession of or is likely to come into the possession of the Data Controller. It also includes any expression of opinion about an individual and any intentions of the data controller or any other person in respect of the individual. It is information that tells something about an individual such as hobbies, lifestyle or family life. It is not always necessary to know an individual's name for data to be personal, a photograph or description of a person can be personal data.

3.1.2. **Sensitive personal data** - is different from ordinary personal data such as name, address, telephone number subject to much stricter conditions of processing. It is data which relates to an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. The presumption in respect of sensitive personal data is that because information about these matters is likely to be of a particularly sensitive nature it needs to be treated with greater care than other personal data. This is particularly so as the loss, theft or mishandling of this category of information is likely to be of a greater detriment to the individual than the loss, theft etc. of other categories of personal data. The nature of the data is also a factor in deciding what security measures are necessary to protect the information.

3.1.3. **Data Controller** - means a person who determines the purpose for which and the manner in which any personal data are, or are to be, processed. Newark and Sherwood District Council is a Data Controller.

3.1.4. **Data Processor** - means any person or organisation that processes the data on behalf of the Data Controller.

3.1.5. **Data Subject** - means the individual who is the subject of the personal data, it is the individual who can be identified from that data.

3.1.6. **Processing** - means obtaining, recording or holding the information or carrying out any operation on the data including organisation, adaptation or alteration of the information or data; the retrieval, consultation or use of the data; the disclosure of the data and the alignment, combination, blocking, erasure or destruction of the information or data. It is difficult to imagine any activity which does not amount to processing.

3.2. **The Data Protection Principles**

At the heart of the DPA are eight legally enforceable principles which together provide a framework for the handling of personal and sensitive personal information. Everyone who processes personal information must abide by the eight principles.

3.2.1. **Principle 1 – Personal data shall be processed fairly and lawfully.**

Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

3.2.2. **Principle 2 – Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.**

Data obtained for one or more specified purposes must not be used for any other purpose.

3.2.3. **Principle 3 – Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.**

Only the minimum amount of personal or sensitive personal data necessary for a particular purpose should be collected. Information, which is not strictly necessary for the purpose for which it is given or obtained should be immediately deleted or destroyed.

3.2.4. **Principle 4 – Personal data shall be accurate and, where necessary, kept up to date.**

Data, which are kept for any length of time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by the Council are accurate and up-to-date. Completion of an appropriate registration or application form etc. will be taken as an indication that the data contained in it is accurate. Individuals should notify the Council of any changes in circumstances to enable personal records to be updated accordingly. It is the responsibility of the Council to ensure that any notification regarding change of circumstances is noted and acted upon.

3.2.5. **Principle 5 – Personal data shall be kept only for as long as necessary.**
Much of the information the Council collects and uses is subject to statutory retention periods while other information will be retained in accordance with best practice, both of which are set out in the Councils Retention and Disposal Policy and Schedule. The term 'as long as necessary' means that information should only be kept for as long as there is a need. If information is no longer needed it must be deleted or destroyed. All personal data must be disposed of securely, appropriately and confidentially

3.2.6. **Principle 6 – Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.**
The rights of the data subject are explained in paragraph 3.3, below.

3.2.7. Principle 7 – Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.

3.2.8. Principle 8 – Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
Data must not be transferred outside of the European Economic Area (EEA) unless properly recognised safeguards are in place. Staff should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere in the world.

3.3. **The rights of the data subject.**
The DPA give individuals a number of rights in relation to the processing of their personal data. The rights include:

3.3.1. **The right of access to personal data** – The Data Protection Act allows individuals to find out what information is held about them, how it is used and who it will or may be shared with. Individuals also have the right to request a copy of the information held about them. This is known as a Subject Access Request

3.3.2. **The right of rectification, blocking, erasure and destruction** – The Data Protection Act allows individuals to apply to the Courts to order a data controller to rectify, block, erase or destroy personal details if they are inaccurate or contain expressions of opinion which are based on inaccurate data.

3.3.3. **The right to prevent processing likely to cause damage or distress** – A data subject can ask a data controller to stop or request that they do not begin processing data relating to him or her where it is causing, or is likely to cause,

substantial distress to them or anyone else. However, this right is not available in all cases and data controllers do not always have to comply with the request

3.3.4. **Rights in relation to automated decision-taking** – An individual can ask a data controller to ensure that no decision which significantly affects them is based solely on processing his or her personal data by automatic means. There are, however, some exemptions to this. Where the processing of personal data is for the purpose of evaluating matters relating to the individual, performance at work, creditworthiness, reliability or conduct and is the sole basis for any decision significantly affecting that person, they have a right in such circumstances to be informed of the logic involved in that decision-taking process.

3.3.5. **The right to prevent processing for direct marketing** – A data subject can ask a data controller to stop or not to begin processing data relating to him or her for direct marketing purposes.

4. The collection and use of personal data

4.1. Newark and Sherwood District Council collects and uses personal information in many ways. In doing so the Council must meet its legal obligations under the Data Protection Act 1998. In particular:

4.1.1. The Council shall only collect and use personal data where it has legitimate reasons for doing so.

4.1.2. When personal data is collected it should be for one or more specified and lawful purpose and shall not be further processed in any manner incompatible with that purpose.

4.1.3. The personal data collected should be adequate, relevant and not excessive for the purpose for which it is processed.

4.1.4. When personal data is obtained it shall be processed fairly and lawfully and should be accurate and, where necessary, kept up to date.

4.1.5. Securely delete or destroy personal information in line with the Councils Retention and Disposal Policy and Schedule or when no longer required for business purposes.

4.2. **Privacy Notices.**

When collecting personal data the Council will inform individuals why their personal data is being collected and will be open and honest as to how they intend to use it. The Council will not deceive or mislead any individual when obtaining their personal data. The Council will use people's personal data in ways that they would reasonably expect. All individuals collecting personal data, in whatever capacity, on behalf of the Council must ensure that individuals are fully informed. A "Privacy Notice" that complies with the Privacy Notice Code of Practise, issued by the

Information Commissioners Office, must be provided to all individuals from whom the Council collects or may collect personal data.

4.2.1. A Privacy Notice is basically a Notice that informs individuals how the Council will use their personal information and who it may or will share that information with. The wording for Privacy Notices will be different for each case in which personal data is collected. The Notice should be clearly communicated to individuals and should be visible on all application forms etc. so that the individual is fully aware of the intended uses of their personal information. As a minimum a Privacy Notice will inform the individual:

4.2.1.1. Who we are – the identity of the Council unless this is already obvious from the header of a form.

4.2.1.2. What we are going to do with the data – the purpose or purposes for which the information will be used.

4.2.1.3. The legal basis that the Council has for processing this data

4.2.1.4. Who the information may, or will be shared with – state the names of any third parties or other Business Units within the Council the Information may or will be shared with.

4.2.1.5. Where they can get further information about the use of the data – provide details of who the person should contact if they wish to know more about the use of the information, their rights under the DPA or to exercise those rights.

4.2.2. Explicit consent will be obtained where information is to be shared with third parties except where the Council has a statutory responsibility to share that information.

4.2.3. It is the responsibility of all Business Managers to ensure that an appropriate Privacy Notice is provided to individuals when their Business Units collect information on behalf of the Council. All Privacy Notices must be checked by the Information Governance team to ensure they meet the requirements of the DPA and the Privacy Notices Code of Practice. The Information Governance team can provide guidance on all aspects of Privacy Notices.

5. **Security of personal data**

Principle 7 of the DPA places an obligation on the Council to take appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data. Set out below are examples of information security, however, this is by no means an exhaustive list.

5.1.1. **Physical security** - Physical security measures should be in place to protect personal data. Documents containing personal information should be kept in locked filing cabinets, cupboards or drawers. On no account should documents

containing personal information be left unattended, such as left overnight on a desk.

5.1.2. **Hard copy personal information** - Each Business Unit must make sure that it holds a record of what personal data it holds, where it is stored and the storage medium.

5.1.3. **Electronic files** - Computers must not be accessible when unattended. Officers are responsible for safeguarding data by ensuring that equipment is not left logged-on when unattended. Where staff leave their computer station for short periods they should "lock" their computer. This is done by pressing the Ctrl, Alt and Delete Keys simultaneously and then choosing the "Lock Computer" option. To unlock their computer staff should enter their log-in details.

5.1.4. **System and network passwords –** It is the responsibility of all members of staff to ensure that passwords used to access the Councils network and programs are robust and changed on a regular basis. Passwords must never be shared with anyone.

5.1.5. **Sending personal information by email –** Personal information sent by email must be sent securely. There are two methods available;

- via the Public Services Network (PSN) from aa GCSx account allocated to this council to a recipient on PSN with a suitably secure account identifiable by .GCSx .PNN or .NHS within the email address

- to a non PSN email using the Cryptshare plug-in to your Council e-mail account. Cryptshare requires a password to be set when encrypting files. The complexity of the password should reflect the sensitivity of the information being sent. Passwords must never be emailed. The recipient should be asked to acknowledge receipt of the encrypted data, following which the sender should telephone the recipient to provide the password to decrypt the data. Whenever possible telephone calls to the recipient should be made via a main switchboard. Where there is a need to send personal information by email on a regular basis the Information Governance team should be asked for advice.

5.1.6. **Sending large documents or files electronically**- The Council's email facility has a restriction on the size of file that can be sent externally. Similarly, many recipients have restrictions on the file size allowed through their email gateway. Documents of up to 1GB can be placed on a Cryptshare portal and secured through encryption. Further guidance on the use of this facility can be obtained from the Information Governance Team of the ICT Help Desk.

5.1.7. **Sending personal information by fax –** Extra care should be taken when personal information is sent by fax. For example fax numbers should be checked to ensure that the information is being sent to the correct recipient. In addition before sending the information the recipient should be advised the information is being sent. Before leaving the fax machine a check should be

made to ensure that all the information taken to the fax machine is accounted for and none is left in or around the fax machine. The recipient should be asked to acknowledge receipt of the information either by email or fax. Sensitive Personal Data should only be faxed as a last resort.

5.1.8. **Sending personal information by post** – When confidential and sensitive personal data are being sent via post the information should be checked by another member of staff before being sent to ensure it is being posted to the correct recipient and all the documents are accounted for. The level of sensitivity of the information being sent should be used as a guide to determining if the letter should be sent by registered or recorded post.

5.1.9. **Printers and copiers** – When sending personal information to a printer the Secure Printing function must be used at all times, irrespective of the level of sensitivity of the information being printed. Details of how to set up and use the Secure Printing function are available on the ICT pages of the Council's intranet site. After printing checks should be made to make all the pages sent to the printer have been picked up. If the printer is out of paper at the end of a print job the paper should be replenished to ensure that the print job is complete. The inclusion of page numbers on documents, wherever possible, will make such checks easier to do and more robust.

5.1.10. **Removable storage devices** – Examples of removable storage devices, would include, but not be limited to, devices such as digital cameras and their media (compact flash, SD cards, memory sticks etc.), USB drives (also known as data pens, data sticks or flash drives) and mobile telephones. The Councils ICT security systems will only allow authorised removable storage devices to be used on Council IT equipment.

5.1.10.1. Where there is a requirement for a member of staff to use a removable storage device it will be sourced, purchased and registered to the user by ICT. Approved removable storage devices must only be used for the temporary storage of Council data and/or work related data.

5.1.10.2. The responsibility for the security of the data stored on any removable storage device, irrespective of the source or level of sensitivity of the data, rests with the registered user of that removable storage device. In the event of the loss or theft of a removable storage device the users Business Manager, ICT and Information Governance must be informed as soon as is practicable. As a minimum when reporting the loss or theft of a removable storage device the user should provide a description of the data it contained, the sensitivity and source of any unencrypted data and the

circumstances of the loss or theft. Should the user subsequently recover the removable storage device the users Business Manager, ICT and Information Governance must be informed, including the circumstances of the recovery as soon as is practicable. Removable storage devices recovered after loss or theft must not be used on any Council owned computer until they have been checked and verified safe for use by ICT.

6. **Home or off site working.**

As a general rule, manual and electronic records containing personal data should not be removed from Council premises. Further, any record containing personal data should never be left unattended at any time and appropriate measures should be taken to ensure that it is not left in public places, on public transport or in cars etc.

6.1. It is recognised that there will be occasions where members of staff need to temporarily remove personal data from Council premises as part of their duties, such as visiting people's homes, or for home or off site working. If there is a need to temporarily remove personal data from Council premises for home or off site working, approval must be sought and given by the appropriate Business Manager or other senior member of staff. In all cases where personal information is temporarily removed from Council premises a log should be kept to record the name of the person taking it, a description of the information, the purpose for taking the information, where it is being taken to, the date taken and the date returned.

6.2. When dealing with personal information at home or outside of Council premises the same measures must be applied as if working in the office. The appropriate technical and organisational measures against the unauthorised or unlawful processing of the personal data and against the accidental loss or destruction of, or damage to, personal data. Members of staff are responsible for the security of equipment, software, files and any other information in their possession outside of Council premises. Personal information held outside of Council premises should, wherever possible, be securely locked away when not in use. It is particularly important to ensure that non-authorised personnel, both in the home environment or whilst working off site, cannot gain access to confidential or personal information. If locked storage space is not available within the home then the data, in whatever format should be kept in a room where access can be monitored by the staff member.

6.3. If IT equipment or hardcopy files are carried in a vehicle they should be placed in the boot rather than in public view, and should be removed from the vehicle when the member of staff leaves the vehicle. On no account should any personal data be left in a vehicle overnight, even if the vehicle is parked in a locked garage..

6.4. Remote Access to the Council network must only be made through approved channels. Remote access requirements must be discussed with ICT.
ICT currently supply two remote connection methods, Citrix and direct VPN. No remote connection outside of these methods should be attempted. Direct VPN connection can only be made on Council equipment. If you are unsure how to access Council systems remotely ,or if you should be doing so, contact ICT

6.5. All Council information, irrespective of its location, is subject to the Councils Retention and Disposal Schedule. Personal or confidential information in printed format that is no longer needed for business purposes must not be disposed of using off site or home facilities, it is to be returned to Council premises and disposed of using the Councils confidential waste procedure.

6.6. Any loss, theft, damage or accidental destruction of personal information at an offsite location or home environment must be reported to the users Business Manager, ICT and Information Governance immediately by using the procedure detailed in the Council's Information Security Breach Policy.

6.7. When working off-site, irrespective of location, care should be taken to ensure that:
a) discussions containing personal information cannot be overheard. This includes both mobile phone and home land-line conversations.
b) information cannot be seen by unauthorised people, whether in hard copy format or on laptop, tablet or smartphone screens.
c) personal information is not left unattended and electronic devices are locked.

7. **Data sharing**

In order to carry out statutory functions or to deliver other services to customers, the Council regularly shares information with third parties. This will normally occur where the individual data subject has been informed at the point of data collection via a Privacy Notice (See 4.2). Where the Council regularly share data with a partner agency or a voluntary organisation, there must be an Information Sharing Agreement or a Data Processing Contract. If the requirement to share data is on a one-off basis, then advice should be sought from the Information Governance Team.

7.1 Where the Council sends personal data to an external partner on a regular basis it should, as Data Controller put into place a an appropriate Information Sharing Agreement or Data Processing Contract which determines the legal framework for sharing that data, the limitations on the use of that data and the security measures that should exist. Guidance on this is available from the Information Governance Team

7.2 Where the Council receives personal data on a regular basis from another organisation, that party would normally require us to enter into their Information Sharing Agreement or Data Processing Contract. If you are asked to enter into such an arrangement this must be reviewed by the Information Governance Team.

8. **Privacy Impact Assessment**

   To ensure that all personal data is processed in accordance with the above policy, the Council has a Privacy Impact Assessment Policy and associated guidance giving a toolkit to be used to assess the risk to personal data. This must be used for any new policy or process that is introduced, or where any existing policy or process is amended.

Document Control Table					
Document title	Data Protection Policy				
Version number	3.	**Status**	Approved	**Protective marking**	Official
Originators name	David Clarke		**Job title**	Information Governance Officer	
Business Unit	Customer Services and External Communications				
Section	Information Governance				
Date approved			**Approved by**	CMT	
Date effective			**Next review due**		

Revision and protective marking history

Version	Date	Protective marking	Author	Notes
V1	27 November 2008	Unrestricted	Steve Bramall	Approved Karen White
V 2.01 2.02	2012	Unrestricted	Steve Bramall	Minor revisions –not approved
V2.03	December 2015	Official	David Clarke	
V3	September 2016	Official	David Clarke	Updated to reflect adoption by European Parliament of the General Data Protection Regulation to be effective from May 2018. Full review includes Privacy Notices, Security of Personal Data, Home and Off-site working, Data Sharing and Privacy Impact Assessment Approved CMT 04-10-2016