New Data Protection Laws

A GDPR Toolkit of local councils

February 2018

nalc
National Association of Local Councils

National Association of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk
w: www.nalc.gov.uk

109 Great Russell Street
London WC1B 3LD

Winckworth Sherwood

SOLICITORS AND PARLIAMENTARY AGENTS

t: 020 7593 5000
e: tvitale@wslaw.co.uk
w: www.wslaw.co.uk

Minerva House
5 Montague Close
London, SE1 9BB
DX 156810 London Bridge 6

Contents

PART 1: 3
1. Foreword 3

PART 2: 4
A brief introduction to the GDPR 4
2. Introduction 5
3. Underlying Principles 8
4. The key changes 9
5. Who will be affected? 9
6. A gear shift in risk 9
7. Examples of fines for failure to comply with the new law 10
8. Key Points for councils 10
9. Why are there two privacy notices in Appendix 4? 10
10. What do I need to do about Consent? 10

PART 3: 11
Next Steps 11
Action Plan 12

PART 4: 14
A detailed guide to the GDPR 14
11. Why implement new legislation? 15
12. Consent, Rights and Accountability 15
13. What is the scope of the GDPR? 15
14. Accountability – What is it and how do I comply? 16
15. What is a privacy notice? 16
16. What does GDPR say about data subject rights? 16
17. Lawful basis for processing 18
18. How do I show that I am processing personal data lawfully? 19
19. When can I process 'sensitive personal data' (special category data)? 20
20. What do I need to do if there is a data breach? 21
21. Consent 21
22. Can existing consents be relied on? 22
23. The need to document your data processing 22
24. Do I need to register (notify)? 23
25. Processing personal data about children 23
26. Will you need to appoint a Data Protection Officer? 23
27. CCTV 24
28. Key data - What to keep and for how long 24
29. What about contracts with suppliers and partners? 24
30. What is a Data Protection Impact Assessment (DPIA) and when is it needed? 25

PART 5: 26
Templates, Policies and Notices 26
Appendix 1 – Further Reading 27
Appendix 2 – Sample Personal Data Audit Questionnaire 28
Appendix 3 – Consent Form 31
Appendix 4 – Privacy Notices 32
Appendix 5 – The role of Data Protection Officers 42
Appendix 6 – DPIA Assessment Checklist 44
Appendix 7 – Subject access policy and template response letters. 47
Appendix 8 – Privacy Policy Checklist 52
Appendix 9 – Part A: Checklist of what to include in a security incident response policy. 56
Appendix 9 – Part B: Cybersecurity checklist 59
Appendix 10 – A template of a council's internal register of processing activities 62
Appendix 11 – Winckworth Sherwood Services 63

PART 1:

1. Foreword

1.1 The General Data Protection Regulation ("GDPR") will take effect in the UK from 25 May 2018. It replaces the existing law on data protection (the Data Protection Act 1998) and gives individuals more rights and protection regarding how their personal data is used by councils. Local councils and parish meetings must comply with its requirements, just like any other organisation.

1.2 The GDPR applies to all local councils and also to a parish meeting without a separate parish council because a local council and a parish meeting are public authorities. The GDPR requires councils and parish meetings to appoint a Data Protection Officer ("DPO") (see ***Appendix 5 – The role of Data Protection Officers*** for more information about DPOs). This is confirmed by new data protection legislation currently being debated in parliament. For the GDPR and the new data protection legislation, the definition of public authorities is the same as that used in the Freedom of Information Act 2000 (which includes local councils and a parish meeting constituted under s. 13 of the Local Government Act 1972).

1.3 This GDPR Toolkit provides a number of practical tools to assist councils with GDPR compliance, in the form of an Action Plan Checklist and a data audit questionnaire, in addition to templates for privacy notices and consent forms.

1.4 I hope that you will take time to digest the guidance contained within this GDPR Toolkit and work out the steps you need to take in order to ensure that your council is compliant. We have been supported in producing this GDPR Toolkit by Winckworth Sherwood, a firm of solicitors based in London, Oxford and Manchester. Further details of data protection law advice and services Winckworth Sherwood can offer direct to councils can be found in ***Appendix 11 – Winckworth Sherwood Services***. NALC has negotiated a reduction of 15% from Winckworth Sherwood's usual charge out rates for data protection advice for councils.

1.5 This GDPR Toolkit takes account of the previous legal guidance published by NALC, it summarises key areas and issues and contains templates and tools councils can use to assist compliance with the GDPR. Councils can find details of NALC's legal guidance at ***Appendix 1 – Further Reading***.

1.6 It is important that councils follow this GDPR Toolkit carefully and use the checklist and forms contained within it to ensure the council is compliant with the new law.

1.7 In this GDPR Toolkit, whenever you see text in ***red, bold, underlined, italics, this is a hyperlink***. Click on the link to be taken to the relevant section or Appendix.

1.8 The toolkit is aimed at councillors, council staff and chairs of parish meetings.

1.9 I commend this GDPR Toolkit to all local councils, as a means of providing valuable support in meeting the requirements of new data protection legislation laws.



Jonathan Owen
Chief executive of National Association of Local Councils

PART 2:

A brief introduction to the GDPR

2. Introduction

2.1 The good news is that the GDPR's main concepts and principles are very similar to those contained in the current Data Protection Act 1998. The Information Commissioner's Office ("ICO") will still be the regulator in charge of data protection and privacy issues. Therefore, if you are complying with the current law, much of what you currently do still applies under GDPR. However, there are some changes and additions, so you may have to do some things for the first time and some things differently (these are highlighted below).

2.2 One of the main changes to note is that the GDPR places a much greater emphasis on transparency, openness and the documents you need to keep in order to show that you are complying with the legislation. This is incorporated within the idea of "accountability".

2.3 The GDPR will however impose new burdens on councils and parish meetings, including new reporting requirements and increased fines and penalties. The UK Government has made clear that after Brexit the UK will continue to adopt a similar standard for data protection as set out in the GDPR.

2.4 This GDPR Toolkit contains an ***Action Plan checklist*** (***Action Plan***) which sets out the actions Councils should take to be compliant with the GDPR. It will be helpful to start by carrying out a ***data audit*** - you may be surprised at just how much personal data is stored and processed around the local community. A template questionnaire to help you do this can be found in ***Appendix 2 – Sample Personal Data Audit Questionnaire***.

Glossary: The jargon explained:

Consent is a positive, active, unambiguous confirmation of a data subject's agreement to have their data processed for a particular purpose. Consent must be easy to withdraw and must be freely given, provided on an opt-in basis rather than opt-out.

Data controller is the person or organisation who determines the how and what of data processing.

Data processor is the person or firm that processes the data on behalf of the controller.

Data subject is the person about whom personal data is processed.

Personal data is information about a living individual which is capable of identifying that individual e.g. a name, email address or photo.

Privacy Notice is a notice from a data controller to a data subject describing how personal data will be used and what rights the data subject has.

Processing is anything done with/to personal data (obtaining, recording, adapting or holding/storing) personal data.

Sensitive personal data is also described in the GDPR as 'special categories of data' and is the following types of personal data about a data subject: racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health or condition; sexual life or orientation; genetic data; and biometric data.

2.5 On the next two pages, is a summary of the main differences between the Data Protection Act 1998 and GDPR:

Change	*Detail of Change*	*Impact of Change*
Record Keeping	Each Data Controller must maintain a record of processing activities under its responsibility. Data Processors must also keep a record of the processing activities they carry out on behalf of a Data Controller.	The level of detail is the same as contained in an ICO registration / notification at present and the log can be requested at any time by the ICO. See ***Appendix 10 – A template of a council's internal register of processing activities*** for a template of the log councils should keep.
Privacy Notices	Under the GDPR, privacy notices must contain more information, be more transparent, use clear and plain language, and must be easily accessible.	Privacy notices will need to be reviewed and updated to make them clearer, more transparent and easily accessible. See ***Appendix 4 – Privacy Notices***
Consent	The way consent is obtained will change under the GDPR as individuals have more rights to decide how their data is processed. Where processing personal data is based on consent, the council must be able to evidence the consent. Consent must be by an "opt in" method.	The types of processing activities which require the consent of an individual need to be identified and consents must be captured in a GDPR compliant manner.
Breaches	Data Controllers must report personal certain types of data breaches to the ICO without 'undue delay', and where possible no later than 72 hours after having become aware of the breach. An individual who has suffered damage as a result of a breach can claim compensation from the Data Controller or the Data Processor.	How councils handle data breaches should be reviewed. Training will be required to increase awareness of what constitutes a breach and how to escalate investigations into breaches.
Right of Access (Subject Access Requests)	The time limit to comply with a Subject Access Request ("SAR") has been reduced from 40 calendar days to one calendar month. The ability to charge £10 per SAR has been removed so all SARs are free of charge from 25th May 2018.	The SAR process will need to be reviewed and updated accordingly.
Data Privacy Impact Assessments ("DPIA")	The GDPR makes it mandatory for DPIAs to be carried out in certain situations. DPIAs will need to contain a description of the processing and the purpose of the processing and need to identify any risks to the personal data and the rights and freedoms of individuals, and the measures and safeguards implemented to mitigate these risks.	DPIAs will need to be introduced where new technologies are used (e.g. CCTV or other monitoring) for high risk data processing activities (e.g. large scale processing of sensitive personal data) or when there are systematic and extensive activities which use automated processing to evaluate, analyse or predict behaviour (e.g. tracking behaviour on a website). See ***Appendix 6 – DPIA Assessment Checklist***

Change	*Detail of Change*	*Impact of Change*
Privacy by Design	When developing, designing or using services or applications which involve processing personal data, Data Controllers and Processors should adopt internal policies and measures to ensure personal data is protected.	If councils introduce new IT systems or launch new websites which collect personal data these new systems should have data protection controls built into their designs from the outset.
Right to Object to processing	Individuals must be advised of their right to opt out of processing activities, including marketing.	"Unsubscribe" methods will need to be reviewed. Any reasonable requests to object to processing should be stored and evidenced.
Right to Erasure	An individual has a right to request that their personal data is deleted. A Data Controller must delete personal data unless there is a legal obligation to retain the personal data.	Data deletion processes will need to be introduced so that data is not retained indefinitely. It's likely a "data cleansing" exercise will need to be carried out prior to 25th May 2018 so that the council is not storing data it no longer requires or has a need to retain.
Profiling	An individual has the right not to be subject to a decision based solely on "automated processing", including profiling. This is where a computer, or computer software rather than a human makes a decision about an individual.	Activities that rely or use automated decision making need to be identified. Processes need to be put in place to allow, where possible, individuals to object to automated decision making (and e.g. request that a human intervenes to make the decision).
Data Protection Officer	A Data Protection Officer (DPO) will need to be appointed by councils. The DPO should report to the highest level of management (i.e. full council) and must be informed about all data protection issues within the council.	Councils and parish meetings must appoint a DPO. Most clerks and RFOs cannot be designated as a council's DPO because they are unlikely to satisfy all of the requirements of the job. For further information please see ***Appendix 5 – The role of Data Protection Officers***
Right of Portability	The GDPR introduces a new right of data portability. This right allows for the data which an individual provided to the Data Controller to be provided to the individual in a structured format, to allow it to be provided to another Data Controller.	It will be important to understand where the data is being stored and in what format to make it easier to move personal data (and receive personal data from other data controllers).

2.6 The rules relating to how you obtain **consent** will change under the GDPR. This will apply in most cases to local residents but not to personal data which is processed in connection with a person's role in the council. For example, staff and councillors cannot give valid consent because consent has to be "freely given" (and it also can be withdrawn at any time). A staff member or councillor cannot be said to be freely giving their consent, because the balance of power between them and the council is not equal. A staff member or councillor cannot 'choose' to withhold their consent

or to exercise their right to withdraw it. If a staff member were to withdraw consent, this would put the council in an impossible situation, as it would be obliged to continue to process the personal data whilst the individual carries out their role. A councillor does not have a free choice to withhold their consent to the processing of their personal data in connection with the role they are performing in the council. This means that 'consent' is not an appropriate legal basis to process personal data for staff or councillors. See paragraph ***17 below*** for more information on the lawful basis local councils can rely on to process personal data under the GDPR.

2.7 You will need to produce two types of Privacy Notice: one for residents (a 'General Privacy Notice') and one for staff, councillors and other role holders. If you have a website, it is good practice to make the General Privacy Notice available online so people can access it. We provide a sample of both Privacy Notices in ***Appendix 4 – Privacy Notices***. You can amend and adapt the templates to produce your own Privacy Notices.

2.8 The General Privacy Notice should be issued to local residents with whom you communicate regularly – perhaps by receiving correspondence, sending a newsletter or undertaking surveys/local consultations. It is important that you collect signed copies of the Consent Form which goes with the General Privacy Notice. If you have an interactive website, you may also be able to collect this consent electronically, so long as the Privacy Notice is clearly made available and the data subject has elected to give consent, such as by expressly ticking a checkbox. The staff, councillors and other role holders Privacy Notice does not need to be signed but should be issued to anyone holding a role in your council to make them aware of the processing that may take place.

2.9 Finally, whilst you may rely on consent for most of your communications, there will be some data processing you will want to do as part of normal council management for which you will not need to gain specific consent for that particular action - holding lists of councillors, managing allotment tenants or contractors/suppliers, undertaking payroll and HR functions for example. In April 2017 the ICO issued some draft guidance on consent for consultation and recommended that consent should be relied on sparingly. There may be other legal grounds available and you should consider consent as 'the last resort' particularly as it can be easily withdrawn.

3. Underlying Principles

3.1 The GDPR has a number of underlying principles. These include that personal data:

(a) Must be processed lawfully, fairly and transparently.

(b) Is only used for a ***specific processing purpose*** that the data subject has been made aware of and no other, without further consent.

(c) Should be ***adequate, relevant and limited*** i.e. only the minimum amount of data should be kept for specific processing.

(d) Must be ***accurate*** and where necessary ***kept up to date***.

(e) Should ***not be stored for longer than is necessary***, and that storage is safe and secure.

(f) Should be processed in a manner that ensures ***appropriate security and protection***.

4. The key changes

4.1 Changes to ***how consent can be obtained*** from data subjects for the use of their data. For example, data subjects have to explicitly 'opt in' to allowing their data to be shared, and it must be made clear for what purpose their data is being used.

4.2 Data subjects have ***new rights***, such as data portability and the right to be forgotten.

4.3 ***Data must only be used for the purpose it was gathered for*** and should be deleted when it is no longer needed for that purpose.

4.4 Sanctions over ***sharing data outside the European Economic Area ("EEA")*** will be strengthened. This requires councils to ensure appropriate privacy safeguards are in place with organisations (e.g. a business hosting and maintaining the council's server) holding data outside the EEA or that the 'importer' of data is on a list of countries which the European Union has deemed to have adequate protection for citizens regarding data protection.

4.5 All councillors, managers and other relevant staff ***must have suitable training*** and awareness as well as additional sources of guidance and support when required.

4.6 Conducting ***Data Protection Impact Assessments*** (DPIAs) in order to design data privacy into any new systems and processes will often be mandatory e.g. if new technology is deployed, where there is processing on a large scale of 'sensitive personal data', or if profiling is performed which will have an impact on individuals.

4.7 Councils and parish meetings will need to appoint a ***Data Protection Officer***.

4.8 ***Data breaches must be reported*** (where this is required) to the ICO ***within 72 hours*** of the breach.

4.9 A new principle of ***accountability*** puts the compliance burden on councils, requiring them to produce and maintain documents that demonstrate what actions have been taken to achieve compliance.

5. Who will be affected?

5.1 The quick answer is every organisation in the UK that handles personal data including all local and public authorities. The GDPR applies to the personal data of individuals living in the EEA and also to the export of personal data to countries outside the EEA.

5.2 The GDPR applies to data controllers (people who specify how and why personal data is processed) and data processors (those who carry out the processing on behalf of the data controllers). Controllers must ensure that their processors comply with the legislation and the processors must also keep records of their processing activities. The new law means that both parties face a higher level of liability than they do under the existing law.

6. A gear shift in risk

6.1 The huge increase in fines (from £500,000 in the UK to the greater of £17 million or 4% of global annual turnover) places significantly additional risk on councils. The GDPR will allow users to claim damages e.g. where there has been a data breach or where processing of data is unlawful.

6.2 It is worth remembering that additional costs may be incurred too. For example, a GDPR breach could require councils to spend substantial time, money and effort to respond to requests for access to personal data, enforcement notices, and minimising any negative publicity.

7. Examples of fines for failure to comply with the new law

7.1 For a failure to appoint a DPO, get parental consent where personal data are collected about a child in the process of providing an "information society service" (e.g. online magazine/newspaper, buying/selling online) a fine of up to the greater of £8.5 million or 2% of the data controller's annual worldwide turnover.

7.2 For a failure to provide adequate information to data subjects or to allow subject access, or to comply with the right of erasure, a fine of up to the greater of £17 million or 4% of the data controller's annual worldwide turnover.

8. Key Points for councils

8.1 Consent for one type of data processing does not give councils permission to do anything else with the personal data e.g. a resident consents to be added to a newsletter mailing list and their details are used for a different purpose such as promoting the facilities of the council. Where councils collect consents e.g. to be added to an email mailing list, these consents will need to be recorded. Councils may need several different consent forms (or elements within a single form) to cover different areas of data processing within the activities of the council.

8.2 Whilst the GDPR removes the requirement for data controllers to register with the ICO, councils will need to pay an annual "data protection fee".

9. Why are there two privacy notices in Appendix 4?

9.1 For staff, volunteers, and councillors, councils should not rely on consent because under GDPR (and the present law) consent must be freely given. As it is necessary to process certain personal data for these staff, councillors and other role holders to allow them to perform their roles, and the balance of power between them and the council is unequal, consent cannot be said to be 'freely given'.

9.2 We have designed two types of Privacy Notice for staff, councillors and other role holders and non role holders and you can find these in ***Appendix 4 – Privacy Notices***. We have designed the Privacy Notices so that one notice can be sent to each individual. The council will not have to send a separate Privacy Notice unless they start using personal data for a purpose not listed in the Privacy Notice or start sharing personal data with a third party not listed in the notice.

10. What do I need to do about Consent?

10.1 If you currently have consent from residents e.g. to send them newsletters or to otherwise keep them informed about council services, facilities or activities, then depending on how it was obtained, it is likely that you will need to obtain a new consent because the rules on obtaining consent under the GDPR are very prescriptive making it harder to obtain it. The consent language set out in ***Appendix 3 – Consent Form*** complies with the new requirements of the GDPR. Councils can start using this straight away for residents whose consent you have not yet obtained. For all existing residents and other members of the community that you currently regularly make contact with, you should also send out the Consent Form in ***Appendix 3 – Consent Form*** to "refresh" or renew their consents. Please remember not to use the Consent Form for staff, councillors and other role holders.

PART 3:

Next Steps

1. Work through the ***Action Plan*** checklist set out overleaf in this section. This sets out a detailed step by step plan to help you ensure compliance.

2. Review what personal data you hold, how you store it, and what basis you have for processing it. Use the Questionnaire in Appendix 2 on page ***28***. This will help you map what personal data you process and where it is.

3. Review and refresh your existing consents and obtain new consents well before May 2018. Start using the Consent Form in Appendix 3 on page ***31*** for collecting new data, and send it to all existing residents except those who are staff, councillors and other role holders.

4. Develop Data Privacy Notices. Use the templates in Appendix 4 on page ***32*** privacy notices for staff, councillors and other role holders and non-role holders in your council.

5. Review the role of the Data Protection Officer. See the description and checklist in Appendix 5 on page ***42***.

6. Use the Data Protection Impact Assessment (DPIA) checklist in Appendix 6 on page ***44*** to help you decide where you will need to carry out a DPIA. Please note you will not usually need to carry out a DPIA for existing systems or processes unless you upgrade or substantially overhaul these.

7. Update your data subject access policy in line with Appendix 7 on page ***47*** where you will also find sample response letters

8. Update your data protection policy. You will find a checklist and sample policy at Appendix 8 on page ***52***.

9. Review your procedures for responding to a security breach and consider your security generally particularly cyber security. See: Appendix 9 on page ***56***.

10. Start keeping a log of what data the council processes. See Appendix 10 on page ***62***.

If you would like additional legal support from Winckworth Sherwood, NALC has negotiated reduced rates for NALC members obtaining data protection advice from Winckworth Sherwood. See Appendix 11 on page ***63*** for more information

Action Plan

You should work through the steps in the Action Plan below. You may not complete all of the steps by 25th May 2018 when the GDPR comes into force but you should have a plan in place by then to complete the remaining steps.

1.	***Raise awareness –*** Councillors, staff, and volunteers, should be made aware that the law is changing. Ensure they undergo training, and that records are kept. They need to know enough to make good decisions about what you need to do to implement the GDPR. ***Decide who will be responsible for the council's compliance with data protection law –*** All councillors, staff, committees and sub- committees are expected to apply data protection legislation in their work. The DPO should have access to full council and relevant staff, committees and sub-committees.
2.	***Data Audit –*** If you do not know what personal data you hold and where it came from you will need to organise an audit to find out. This means reviewing personal data held on staff and volunteers, people using council facilities or services, councillors, contractors, residents, and more. You should document your findings because you must keep records of your processing activities. You should also record if you share data with any third parties. See ***Appendix 2 – Sample Personal Data Audit Questionnaire***
3.	***Identify and document your 'lawful basis' for processing data –*** To legally process data under the GDPR you must have a 'lawful basis' to do so. For example it is a lawful basis to process personal data to deliver a contract you have with an individual. There are a number of different criteria that give you lawful basis to process and different lawful basis give different rights to individuals.
4.	***Check your processes meet individuals' new rights –*** The GDPR will give people more rights over their data. For example, the GDPR gives individuals the right to have personal data deleted. Would you be able to find the data and who would be responsible for making sure that happened? Ensure you have the systems in place to be able to deliver the 8 rights. ***Know how you will deal with 'subject access requests' –*** Individuals have the right to know what data you hold on them, why the data is being processed and whether it will be given to any third party. They have the right to be given this information in a permanent form (hard copy). This is known as a 'subject access request' or "SAR". You need to be able to identify a SAR, find all the relevant data and comply within one month of receipt of the request. Under the GDPR the time limit for responding to SARs is reduced from 40 days to one calendar month and the £10 fee is abolished.
5.	***Review how you get consent to use personal data –*** If you rely on consent as your lawful basis for processing personal data, then you need to review how you seek and manage consent. Under the GDPR consent must be freely given, specific and easily withdrawn. You can't rely on pre-ticked boxes, silence or inactivity to gain consent instead people must positively opt-in. See our consent language in ***Appendix 3 – Consent Form***
6.	***Update your Policies & Notices –*** Have clear, practical policies and procedures for staff to follow, and monitor their operation. ***Privacy Notices -*** You must tell people in a concise, easy to understand way how you use their data. You may well already have privacy notices but they will all need to be updated. Under the GDPR privacy notices must give additional information such as how long you will keep data for and what lawful basis you have to process data. See ***Appendix 4 – Privacy Notices*** ***Data Retention & Disposal –*** Ensure you update your data retention policy and inform all data subjects how long you will retain data. When disposing of records and equipment, make sure personal data cannot be retrieved from them. ***Websites –*** Control access to any restricted area. Make sure you are allowed to publish personal data (including images) on website/social media. ***Data sharing –*** Be sure you are allowed to share personal data with others and make sure it is kept secure when shared. ***CCTV –*** Inform people what it is used for and review retention periods. Ensure you have the correct signage on display and a suitable policy in place. ***Training –*** Train staff on the basics of personal data security, where the law and good practice need to be considered, and know where to turn for advice.

7. ***Build in extra protection for children*** – The GDPR says children under 16 cannot give consent (although this will be reduced to 13 in the UK) so you will have to obtain consent from a parent or guardian. You will need to be able to verify that person giving consent on behalf of a child is allowed to do so. Privacy notices should to be written in language that children can understand.

8. ***Update your contracts to deal with processing by others –*** Recognise when others are processing personal data for the council and make sure they do it securely. You will need to ensure your contracts are updated to include the GDPR required clauses and put in place an audit programme to supervise them. Consider also how you select suppliers. There must be a written contract which imposes these obligations on processors:

1. Follow instructions of the controller.
2. Ensure their personnel are under a duty of confidence.
3. Keep the personal data secure.
4. Allow the controller to consent to sub-contractors.
5. Flow down obligations to sub-contractors (but remain responsible for actions of the sub-contractor(s).
6. Assist the controller when individuals exercise their rights to access, rectify, erase or object to processing of data.
7. Assist the controller with privacy impact assessments.
8. Assist the controller with security and data breach obligations and notify the controller of any personal data breach.
9. Return or delete data at the end of the agreement (but can keep a copy).
10. Demonstrate compliance with these obligations and submit to audits.
11. Inform the controller if their instructions would breach the law.

9. ***Personal Data Breaches - Get ready to detect report and investigate these -*** A data breach is a breach of security leading to 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'. You will need to have the right procedures in place to detect, investigate and report a breach. The GDPR introduces a duty to report certain types of data breaches to the ICO and in some cases to the individuals concerned. You need to be able to demonstrate that you have appropriate security, technical and organisational measures in place to protect against a breach. If there is no risk of harm to an individual (for example because some low risk data has been inadvertently released or made public such as an email address) then this type of breach would not need to be reported. Unauthorised access to data that could be used to steal someone's identity such as their banking data must be reported.

- The DPO should be involved after the council becomes aware of a data breach.
- Councillors, staff, contractors and the council's data processors should be briefed on personal data breach avoidance, and on what to do in the event that a breach occurs.
- Examples of personal data breaches and steps to avoid them include:
  - Emails and attachments being sent to the wrong person, or several people – it is easy to click the wrong recipient. Slow down, check thoroughly before clicking 'send'.
  - The wrong people being copied in to emails and attachments. – Use BCC (Blind Carbon Copy) where necessary.
  - Lost memory sticks which contain unencrypted personal data – The council should put protocols in place for memory stick usage
  - Malware (IT) attach – ensure up to date anti-virus software is in place.
  - Equipment theft – check security provisions.
  - Loss of personal data which is unencrypted

10. ***Build data protection into your new projects -*** Privacy by design means building data protection into all your new projects and services. It has always been good practice, but the GDPR makes privacy by design an express legal requirement. To achieve this, data protection impact assessments should be undertaken where new technology is being deployed, where profiling may significantly affect individuals or sensitive categories of data will be processed on a large scale. Clarify who will be responsible for carrying out impact assessments, when you will use them and how to record them. See our DPIA assessment checklist in ***Appendix 6 – DPIA Assessment Checklist***.

11. ***Appoint your Data Protection Officer.*** See ***Appendix 5 – The role of Data Protection Officers***

PART 4:

A detailed guide to the GDPR

11. Why implement new legislation?

11.1 The GDPR is not intended to restrict the processing of personal data, but rather align it to the modern digital world and ensure that such processing is done in a way that protects the data subject's rights.

12. Consent, Rights and Accountability

12.1 From May 2018, some residents may need to give their consent before you send them communications – see paragraph 21 - ***Consent*** for more information. This will need to be clear and unambiguous - some form of positive action to 'opt-in'. You will need to gather this consent. We have included a ***Consent Form*** to go with the template General Privacy Notice but you can include the consent language in other forms you use.

12.2 Data subjects have a number of rights, including to be told how personal data is used by the data controller, to know what data is held about them, to correct any errors and the right 'to be forgotten' under certain circumstances. Data controllers, such as a council, will need to make provision for people to exercise these rights.

12.3 The GDPR introduces a stronger requirement on accountability for data controllers. This means that you must be able to show that you are complying with the principles by providing evidence.

13. What is the scope of the GDPR?



13.1 Many of the existing core concepts under the current law are reflected in the GDPR. Familiar concepts of personal data, data controllers and data processors are broadly similar in the current law and the GDPR. Currently there is a very broad definition of 'processing' and this captures the retrieval, management, transmission, destruction and retention of personal data. This will continue to be the case under the GDPR.

13.2 Organisations which are not in the European Economic Area ("EEA") will still have to comply with the GDPR. Non-EEA organisations that operate in the EEA with EEA data subjects' personal data should designate a representative in the EEA, as a point of contact for supervisory authorities (who are responsible for ensuring compliance with the GDPR) and data subjects. In the UK the supervisory authority is the ICO.

What's new? Legal rights of Data Subjects	
DPA 1998	**GDPR/ new (UK) data protection legislation**
Under the current law a Data Subject can request a copy of their data (Subject Access Request) on payment of a nominal fee and has a common law right of erasure or rectification of their personal data.	**Under the GDPR, these rights are explicit and no longer require a fee. In addition, there is a right to have personal data extracted in an electronic portable format that will allow switching between different service providers. There are new rights to erase data too (if it is no longer needed).**

13.3 Both UK and international organisations will need to understand how data flows within the organisation and outside particularly when the data crosses international borders.

13.4 Councils should review their current policies and procedures in place in light of the flow of data within the council.

Under the GDPR, personal data now includes information relating to a living person, who can be identified directly or indirectly by such information (e.g. name, ID number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic or social identity of that person). Under the GDPR, sensitive personal data (which has a higher threshold of protection) will include genetic data, biometric data and data concerning sexual orientation, in addition to the previous categories such as religious belief, race/ethnic origin, trade union membership, and health.

14. Accountability – What is it and how do I comply?

14.1 The new accountability principle means that you must be able to show that you are complying with the principles set out ***on page 8*** of this GDPR Toolkit. In essence, you cannot just state you are compliant; you have to prove it and provide evidence. To do this there are a number of actions you should take, such as documenting the decisions you take about your processing activities and various other ways that show compliance - such as attending training, reviewing any policies and auditing processing activities.

15. What is a privacy notice?



15.1 The transparency requirements under the GDPR require councils to provide individuals with extensive information about how their personal data is collected, stored and used. This information must be easily accessible, transparent and presented using clear and plain language. In practice, this means that councils will need to include more information in their privacy policies, as well as retaining more detailed records of their data processing activities in relation to their staff, customers and third parties.

16. What does GDPR say about data subject rights?

16.1 The revised data subject rights under GDPR may present practical issues for councils, especially where personal data is spread across multiple or complex systems. Councils will need to update the relevant policies and procedures to reflect the new the GDPR requirements. You should review existing procedures in place when responding to data subject access requests to ensure the new time scales can be met.

16.2 Generally, the rights of individuals that are granted under the GDPR are the same as under the current law but with some significant additions. The GDPR includes the following rights for individuals:

(1) **The right to be informed**

(A) Individuals continue to have a right to be given "fair processing information", usually through a privacy notice. Under the GDPR there is additional information that you will need to supply.

(B) For example, you will have to explain the lawful basis for the processing of their data; your data retention periods (how long you keep it for) and that individuals have a right to complain to the ICO if they think that there is a problem in the way that you deal with their personal data.

(2) **The right to access (includes subject access requests)**

(A) Under the GDPR the right of data subjects to request information about the personal data processed by councils remains largely the same. However, under the new regime councils must respond without undue delay and in any case within one calendar month of receipt of the request.

(B) Additionally, the £10 fee for making a request will be abolished which is likely to lead to a greater number of requests. It is estimated that 25% of requesters at present withdraw or do not pursue their request when asked to fill in a form and pay the current £10 fee. Councils will need to consider if they have sufficient resources to deal with an increase in the volume of data subject access requests.

(C) You will be able to refuse or charge a "reasonable fee" for requests that are manifestly unfounded, excessive or repetitive. If you do refuse a request you must tell the individual why and that he/she has the right to complain to the ICO or go to court.

(3) **The right to rectification (correction)**

(A) Individuals have the right to have their personal data corrected (rectified) if it is inaccurate or incomplete. If the data has already been given to third parties, you must tell those third parties of the correction. You must also tell the individuals about the third parties to whom the data has been given.

(4) **The right to erasure (also known as the right to be forgotten)**

(A) Data subjects have the right to request the removal or erasure of their personal data, for example if it is no longer necessary to process their data, the individual objects to such processing and/or the individual withdraws consent. Not only will councils need to comply with such requests but they will also need to ensure that any third party with whom the data was shared also deletes such data.

(B) This does not mean that a person can immediately request that his/her personal data is deleted. If the purposes for which the data was collected still exist, then a person will not be able to request the deletion of that data, unless it was given by consent and they are withdrawing their consent. This is one reason why consent is not the best lawful basis for data processed in connection with a person's role in the council.

(5) **The right to restrict processing**

(A) Individuals have the right to restrict processing of their personal data in certain circumstances (for instance if a person believes his/her personal data is inaccurate or he/she objects to the processing). If

processing is restricted, you can still store the data but cannot otherwise use the data.

(6) **The right to data portability**

(A) Data subjects will have the right to request that their personal data be provided to them (or a third party) in a machine readable portable format free of charge. Councils should consider how and where the personal data is held and if such data can be easily transferred in a safe, secure manner without impacting the usability of such data by the data subject. The council will need to comply with such requests without undue delay, and in any event within one month.

(B) This is a new right introduced by the GDPR. Individuals have the right to obtain and reuse personal data for their own purposes across different services. It allows them to move, copy, or transfer personal data easily from one IT system to another.

(7) **The right to object**

(A) Individuals have the right to object to processing in certain circumstances e.g. if a council has relied on one lawful ground to process data without consent and an individual is not happy with this they have the right to object to the council processing their data.

(8) **The right not to be subject to automated decision-making including profiling**

(A) The GDPR provides protection against the risk that a potentially damaging decision is taken without human intervention. This right is similar to that contained in the DPA.

17. Lawful basis for processing

17.1 The GDPR sets out ***six lawful bases*** for processing data. Unless an exemption applies, ***at least one of these will apply in all cases***. It is possible for more than one to apply at the same time. One of the new requirements for Privacy Notices is that you must set out in the Privacy Notice which Lawful basis you are relying on. In the sample notices in ***Appendix 4 – Privacy Notices*** you will notice that we have opted to rely on more than one lawful basis. For most councils, the relevant ones will be: 1 – Consent (but not for staff, councillors and other role holders), 2 – compliance with a legal obligation (which includes performance of statutory obligations), 3 – Contractual necessity (for example with contractors), etc. Slightly different lawful bases apply in each of the sample Privacy Notices as some will only apply to staff, councillors and other role holders.

17.2 In many situations, more than one lawful basis may apply. For example a council may be processing personal data about a staff member in connection with an employment contract and at the same time have a legal obligation to process the same personal data.

17.3 The six lawful bases for processing personal data under the GDPR are:

(1) **Consent**

- A controller must be able to demonstrate that consent was given. Transparency is key: consents given in written declarations which also cover other matters must be clearly distinguishable, and must be intelligible, easily accessible and in clear and plain language.

- Consent is defined as any freely given, specific, informed and unambiguous indication of the data subject's wishes – either by a statement or by a clear affirmative action.

(2) **Legitimate interests**

- This involves a balancing test between the controller (or a third party's) legitimate interests and the interests or fundamental rights of and freedoms of the data subject – in particular where the data subject is a child. The privacy policy of a controller must inform data subjects about the legitimate interests that are the basis for the balancing of interests.

- Please note, councils and parish meetings are public authorities and under the GDPR public authorities cannot rely on legitimate interests as a legal basis for processing personal data.

(3) **Contractual necessity**

- Personal data may be processed if the processing is necessary in order to enter into or perform a contract with the data subject (or to take steps prior to entering into a contract).

(4) **Compliance with legal obligation**

- Personal data may be processed if the controller is legally required to perform such processing e.g. complying with the requirements of legislation.

(5) **Vital Interests**

- Personal data may be processed to protect the 'vital interests' of the data subject e.g. in a life or death situation it is permissible to use a person's medical or emergency contact information without their consent.

(6) **Public Interest**

- Personal data may be processed if the processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.

17.4 Which lawful bases apply to councils?

(a) As set out above, for most councils a number of different lawful bases will apply at the same time. Often councils will be performing a task in the public interest, under a legal obligation e.g. processing data in the exercise of a statutory power and sometimes as a result of contractual necessity.

18. How do I show that I am processing personal data lawfully?

18.1 For example, the lawful basis for processing the personal data contained in planning applications is 'compliance with a legal obligation' This is because this processing activity is a requirement of legislation. However, disclosure of a person's details to a third party may require the individual's consent.

19. When can I process 'sensitive personal data' (special category data)?

19.1 Sensitive personal data, which the GDPR refers to as 'special category data', means information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health, and sexual life. The GDPR adds the following new additional categories: genetic data, biometric data and sexual orientation. To process sensitive personal data one of the following should apply – however please note that:

(a) More than one of the criteria below can apply at the same time.

(b) Data controllers need to establish a lawful basis for processing any personal data (see previous paragraph ***Lawful basis for processing***) and, if they are processing sensitive personal data they must also establish that ***at least one*** of the criteria below applies:

(i) ***Explicit consent*** of the data subject has been obtained (which can be withdrawn).

(ii) ***Employment Law*** – if necessary for employment law or social security or social protection.

(iii) ***Vital Interests*** – e.g. in a life or death situation where the data subject is incapable of giving consent.

(iv) ***Charities, religious organisations and not for profit organisations*** – to further the interests of the organisation on behalf of members, former members or persons with whom it has regular contact such as donors. Please note councils and parish meetings cannot rely on (iv) as a lawful basis for processing personal sensitive data.

(v) ***Data made public by the data subject*** – the data must have been made public 'manifestly'.

(vi) ***Legal Claims*** – where necessary for the establishment, exercise or defence of legal claims or for the courts acting in this judicial capacity.

(vii) ***Reasons of substantial public interest*** – where proportionate to the aim pursued and the rights of individuals are protected.

(viii) ***Medical Diagnosis or treatment*** – where necessary for medical treatment by health professionals including assessing work capacity or the management of health or social care systems.

(ix) ***Public Health*** – where necessary for reasons of public health e.g. safety of medical products.

(x) ***Historical, Statistical or scientific purposes*** – where necessary for statistical purposes in the public interest for historical, scientific research or statistical purposes.

19.2 In a council context the most relevant lawful basis for processing under Special Category Data are likely to be (i), (ii) and (vii), namely:

- Explicit consent from a person; or
- Employment law (for staff);
- Reasons of substantial public interest (in performing the public authority role of the council)

20. What do I need to do if there is a data breach?

20.1 A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Currently, data breaches do not have to be routinely notified to the ICO or others (although the ICO recommends that it is good practice so to do). The GDPR makes informing the ICO and the individuals affected compulsory in certain circumstances e.g. where there is a high risk to the individuals involved, for instance, through identity theft.

What's new? Notifying breaches	
DPA 1998	**GDPR/ new (UK) data protection legislation**
Currently the notification of breaches to the ICO is effectively voluntary.	**The GDPR introduces a new obligation to notify certain breaches to the ICO within 72 hours and in some cases data subjects will have to be notified too.**

20.2 More details can be provided after 72 hours, but before then the ICO will want to know within that time the potential scope and the cause of the breach, mitigation actions you plan to take, and how you plan to address the problem.

Under the GDPR, councils will be required to report a personal data breach, which meets the reporting criteria, within 72 hours to the Information Commissioner. In line with the accountability requirements, all data breaches must be recorded along with details of actions taken. Councils should ensure that there is a person, or a group of people, who are responsible for dealing with any data breaches which may occur , outline a response plan and set out a procedure detailing how, when and to whom data subjects should report data breaches.

21. Consent

21.1 Where you rely on consent as the lawful basis for processing any personal data, you need to be aware that to be valid under the GDPR, consent must be freely given, specific, informed, unambiguous and able to be withdrawn. Also, you will need to record how and when the consent was obtained (and review this over time). Consent will require "clear affirmative action". Silence, pre-ticked boxes, inactivity, or a history of processing without complaints will not constitute consent.

21.2 Therefore, if you wish to rely on consent, you will have to make sure that any consent wording is sufficiently strong to allow you to show that the consent given is unambiguous and the person knows exactly to what he/she is consenting. You will also have to tell individuals that they have the right to withdraw consent at any time and ensure that the procedure for withdrawing consent is just as simple as granting consent e.g. by sending an email or un-ticking a box.

21.3 For example, you cannot use personal data from the electoral roll provided to the council by the principal authority to send mail to individuals about activities of the council without seeking consent first. If you have not obtained consent from individuals to do this, you will not be able to use their personal data in this way. You will need to keep records of all consents received and periodically review them e.g. every 5 years to ensure that they are still valid.

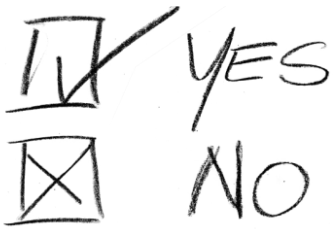
21.4 You should note that consent may not be appropriate in every case. Remember there are other lawful bases for processing personal data.

22. Can existing consents be relied on?

22.1 You may need to review any existing consents you have on record to check whether they comply with the stricter rules under the GDPR. The basic rule is that if consent would have been valid under the soon-to-commence GDPR you can rely on it but if the consent was obtained using an opt-out box or is ambiguous you cannot rely on it after 25 May 2018.

22.2 Under the GDPR ***consent must be unambiguous***. Consent to process sensitive personal data must be explicit, however, consent to process other types of personal data does not need to be explicit. Consent must, however, still be specific, informed and active: silence or inactivity is not sufficient.

22.3 ***Consent must be freely given and individuals must be able to withdraw consent*** (without detriment). Entering into a contract, or receiving a service, should not be 'tied' to the user giving consent to the processing of data which is not, in fact, necessary for the service to be delivered. Councils must also seek separate consents for separate processing operations. There is a presumption that these types of forced or generic consents will not be valid: Councils will need to change the language they use to obtain consent so that the council can demonstrate the consent was freely given, specific, informed, and unambiguous.



What's new? Marketing consents	
DPA 1998	**GDPR/ new (UK) data protection legislation**
Under current law an opt-out can be relied on by data controllers for gaining marketing consent (for example, tick here if you don't wish to receive offers, etc.).	**Under the GDPR, marketing consent must be explicit and in a form of:** ▪ **time limited opt-in** ▪ **in plain language** ▪ **easy way to opt-out and to say no to profiling** **If consent can't be proved, a council could face a big fine under the GDPR and an Enforcement Order to stop processing personal data.**

22.4 Processing does not need to be based on consent: other bases for processing still exist, including contractual necessity, compliance with a legal obligation

22.5 The Information Commissioner has recently published draft guidance on consent under the GDPR. This sets out that it is unlikely that an employer will be able to show that a staff member has given valid consent under the GDPR (i.e. that it has been freely given) and employers should therefore rely on one of the other conditions for processing rather than consent.

23. The need to document your data processing

23.1 Controllers and processors must keep and make available to supervisory authorities. (in the UK, the supervisory authority is the ICO) very comprehensive records of data processing which in turn requires councils to start work on detailed data mapping exercises to determine what data is collected, how and why, where it is stored, who has access to it and whether there is a legal justification to process it.

24. Do I need to register (notify)?

24.1 The need for data controllers to register/notify with the ICO is removed under the GDPR. Nevertheless, it is important that you look at the various types of data processing you carry out, identify the purposes and legal basis for this processing and keep a written record of all your processing activities, security measures and data retention practices. Such information may need to be supplied to the ICO if requested.

24.2 However, the Data Protection Bill (currently before Parliament) allows the Secretary of State to make regulations requiring data controllers to pay a charge to the ICO and to provide information to the ICO to help the ICO identify the correct charge to be levied.

24.3 The ICO has confirmed that although there is no requirement to register/notify under the GDPR, there will be a new annual "data protection fee" which data controllers will be legally required to pay. The amount as yet has not been finalised but will depend on the size of the organisation, its annual turnover and the amount of personal data it processes.

24.4 The ICO has stated that the new fee system will come into existence from 1 April 2018 but until that time data controllers should continue to register/notify as per usual. Once the new system is finalised the ICO has promised to let organisations know.

25. Processing personal data about children

25.1 Under the GDPR itself, parental consent will be required for the processing of personal data of children under age 16. European Union ("EU") Member States may lower the age requiring parental consent to 13. In the draft Data Protection Bill recently published by the UK Government, the UK has adopted this option to reduce the age of consent to 13. This remains subject to Parliamentary approval.

25.2 You should also remember that you have to be able to show that you have been given consent lawfully and therefore, when collecting children's data, you must make sure that your privacy notice is written in a language that children can understand and copies of consents must be kept.

26. Will you need to appoint a Data Protection Officer?

26.1 Data Protection Officers are specifically required in certain circumstances under the GDPR, such as where organisations process sensitive (special category) personal data on a "large scale" or are a public body. As a public body, local councils (and parish meetings) will be required to appoint a DPO, who may be an internal or external appointment In other words, the DPO may be a staff member or engaged under a service contract.

26.2 However most clerks and RFOs cannot be designated as a council's DPO. This is because although they may satisfy some requirements of the DPO job, they will not satisfy all of them. There can also be a conflict of interest between the role of a clerk and RFO and that of a DPO and these types of conflicts should be avoided. More information about the role of DPOs can be found in ***Appendix 5 – The role of Data Protection Officers***.

26.3 The council, as data controller, remains responsible for compliance with the data protection legislation including the GDPR.

26.4 All councillors, staff, committees and sub-committees are expected to apply data protection legislation in their work. The DPO should have access to full council and relevant staff, committees and sub-committees

26.5 Aside from the DPO, the council may wish to appoint a staff member who is able to provide central support and guidance in respect of compliance with data protection legislation. If a staff member is to take on this role, it does not need to be a new member of staff, but may be added to the duties of an existing member of staff. The job title 'Data Protection Compliance Officer' or similar, rather than 'Data Protection Officer' ought to be used, to avoid confusion with the GDPR required DPO, to which specific responsibilities are attached under the legislation.

27. CCTV

27.1 Some councils may have CCTV in place to try to protect the security of buildings. The GDPR does not specifically change the rules about CCTV but the new transparency requirements mean that councils should check whether there are adequate signs erected containing the right level of detail.

What's new? CCTV	
DPA 1998	**GDPR/ new (UK) data protection legislation**
The ICO has a code of conduct for CCTV users which recommends a sign is erected notifying visitors they are being recorded.	**Councils should revisit the signs to ensure full transparency – for example does the sign state that automatic number plate recognition software is used and list all the purposes the data collected will be used for?**

28. Key data - What to keep and for how long

28.1 You need to decide how long to keep information, including register of councillors ' interests and councillor contact details, Electoral Roll, correspondence with residents, information about staff, contractors' details, allotment tenants and a range of other personal data , typically held by councils.

29. What about contracts with suppliers and partners?

29.1 The GDPR requires that all contracts where a company or other organisation supplies goods and services to the council and processes personal data (e.g. a company providing payroll services, CCTV or IT support, etc.) must be in writing and must contain a proscribed list of provisions describing how the data is processed. As data processors are liable directly under the GDPR, councils should expect more lengthy and difficult negotiations with suppliers as they try to address their new exposure under the GDPR. If third party organisations provide the council with services and they can access personal data then this applies to you.

What's new? Contracts with data processors and controllers	
DPA 1998	**GDPR/ new (UK) data protection legislation**
The current law makes contracts compulsory	**The GDPR requires contracts to include certain terms. If councils fail to do this by May 2018 both controllers and processors can be fined.**

29.2 What new provisions must be included? There are eleven in total but here is a sample:

(a) Processors must process data only on the instructions of the data controller.

(b) People authorised to access data are subject to confidentiality.

(c) Ensure security of processing.

(d) Processors must assist the controller in complying with data subjects rights (where possible).

(e) Processors must assist the controller with regard to security measures, breach reporting and DPIAs.

30. What is a Data Protection Impact Assessment (DPIA) and when is it needed?

30.1 A Data Protection Impact Assessment is a type of audit ***used to help assess privacy risks***. A council might carry out a DPIA if it was going to outsource its payroll function for the first time or if it was installing CCTV which included cameras pointed at public areas.

30.2 A DPIA assesses the impact of any proposed processing operation, for example the use of new technology, on the protection of personal data. A DPIA should be carried out before the processing of the personal data starts and then updated throughout the lifetime of any project.

30.3 In ***Appendix 6 – DPIA Assessment Checklist*** there is a DPIA checklist to help you determine whether a DPIA is needed. The Article 29 Working Party, which is an independent agency that advises the European Union on data protection law, recently published guidance on when a DPIA is required. This guidance is reflected in the DPIA Checklist in Appendix 6. It is expected that the ICO will also publish further guidance shortly.

30.4 The content of a DPIA usually includes:

(a) A description of the processing activities and their purpose;

(b) An assessment of the need for and the proportionality of the processing; and

(c) The risks arising and measures adopted to try and prevent any risks, in particular any safeguarding or security measures to protect data and comply with the GDPR.

PART 5:

Templates, Policies and Notices

Appendix 1 – Further Reading

Previous NALC legal guidance on GDPR:

1. L03-17 - Introduction to the GDPR
2. L04-17 - Getting ready for GDPR:
3. L05-17 - GDPR – summary of the main provisions
4. L06-17 - GDPR – Application to Parish Meetings:
5. L07-17 - GDPR – Payment of Fees to the ICO:
6. L08–17 GDPR – Privacy Notices and legal basis for processing data
7. L09-17 - GDPR – Data Subject Access Requests
8. L10-17 - GDPR – Data Protection Officers
9. L02-18 - GDPR – Reporting Personal data breaches

Appendix 2 – Sample Personal Data Audit Questionnaire

A. To be used to help councils with their record keeping obligations under the GDPR.

B. This questionnaire is designed to help councils (and parish meetings) to audit their personal data. It is important that councillors and staff complete this form as comprehensively as possible. The purpose of a data audit is to find out what data the council is processing, what it is used for, where it is located and who has access to it. It is an important step in assessing whether there are any risks in the type of processing the council carries out. For example if the council processes a large amount of sensitive personal data but has no access controls in place restricting who can see or use the data, that is a security risk which needs to be fixed. Without carrying out an audit a council may not know what risks it currently has with data.

C. The generic phrase "council" has been used to refer to the data controller (see glossary below) using the questionnaire.

D. Glossary

- "**Personal Data**" is any information about a living person which can identify them. This is not just someone's name and address but any information which can identify them (directly or indirectly). For example a phone number or email address is personal data. Any other contact information or a person's employment history, or credit history are all personal data.
- **"Data controller"** is the person or organisation who determines the how and what of data processing.
- **"Data processor"** is the person or firm that processes the data on behalf of the controller.
- **"Data subject"** is the person about whom personal data is processed.
- **"Processing"** personal data means storing or deleting any personal data on a computer, database or some manual files (e.g. HR, allotment tenancy files or invoices with contractor payment details). The word 'processing' also covers selecting a name for a mailing list, or reading it off a screen during a call. It includes transferring and altering data. Indeed, practically anything done to personal data constitutes processing.
- **"Sensitive personal data or special categories of personal data"** are any of the following types of personal data about a data subject: racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health or condition; sexual life or orientation; genetic data; and biometric data.

Part A:	**YOUR INFORMATION**	
1.	1. Person completing questionnaire a) Name. b) Role. c) Telephone number. d) Email.	a) ..... b) ..... c) ..... d) .....
2.	Data controller (e.g. name of local council or parish meeting)	
3.	Date you completed this questionnaire	
Part B:	**COMMUNICATING PERSONAL DATA**	
4.	This section relates to communications with councillors, staff and local residents (including mailing lists) general public. **a) What type of personal data does the council keep?** e.g. name, contact details such as bank details. **b) Where does the council get the personal data from?** e.g. staff, residents, other local authorities, charities and sports clubs, community groups, recruitment agencies. **c) Why does the council collect or process the data – what does the council do with the personal data?** For purposes relating to: e.g. local resident concerns, management of council facilities, services and staff, contract management, performance	

	of statutory functions. [*Please list all reasons*]. **d) Who does the council disclose personal data to?** E.g. the public, councillors, staff and contractors carrying out the work of the council, pension providers, HMRC, credit reference agencies, recruitment agencies, prospective employers **e) Do the council or parish meeting minutes contain personal data?** **f) Does the council ever send personal data overseas and if so where to and to which organisation? This might include overseas companies providing database or email services.** e.g. do any of your suppliers use 'cloud storage' and if so do you know where the personal data is located? **g) Does the council collect any sensitive personal data?** see definition above. **h) If so for what reason?** e.g. for safeguarding compliance; physical or mental health data relating to staff; racial and ethnic origin relating to equal opportunities monitoring. [Please list anything else]	
Part C:	**SUPPLIERS, COMPANIES, AND OTHER ORGANISATIONS THE COUNCIL CONTRACTS WITH**	
5.	About individuals or representatives of organisations which supply us with services such as for council repairs, or with whom we are in contact **a) Who does the council keep personal data about?** e.g. tradesman, recruitment agencies, surveyors, architects, builders, suppliers, advisers, payroll processors. [Please list any others] **b) What type of personal data does the council keep?** e.g. name, contact details, qualifications, financial details, details of certificates and diplomas, education and skills. [Please list any others] **c) Where does the council get the data from?** e.g. the individuals, suppliers. [Please list any others] **d) Why does the council collect or process the data?** e.g. council property maintenance and repairs and management of council facilities, pay and manage staff. [Please list any other reasons].	
Part D:	**GENERAL QUESTIONS ABOUT PERSONAL DATA**	
6.	a) How does the council store the personal data collected? b) Does the council take any steps to prevent unauthorised use of or access to personal data or against accidental loss, destruction or damage? If so, what? c) How does the council manage access to data d) What is the process involved in giving access to staff or councillors?	
7.	a) Do any procedures exist for e.g. correcting, deleting, restricting, personal data? If so, please provide details.	
8.	a) Who has access to / is provided with the personal data (internally and externally)? b) Is there an authorisation procedure for accessing personal data? If so, please provide details.	
9.	Does the council provide a copy of all existing privacy notices?	
10.	So far as the council is aware, has any personal data which was gathered for one purpose been used for another purpose (e.g. communicating council news?) If so, please provide details.	
11.	Does the council have any policies, processes or procedures to check the accuracy of personal data?	
12.	a) In the event of a data security breach occurring, does the council	

	have in place processes or procedures to be followed? b) What are these?	
13.	a) If someone asks for a copy of personal data that the council holds about them, i.e. they make a 'subject access request', is there a procedure for handling such a request? b) Is this procedure contained in a written document?	
14.	Does the council have an internal record of the consents which the council has relied upon for processing activities? e.g. to send council newsletters to residents	
15.	a) Are cookies used on our council website? b) Does the council provide information about the cookies used and why they are used? c) Does the council keep a record of the consents provided by users to the cookies? d) Does the council allow individuals to refuse to give consent?	
16.	Does the council have website privacy notices and privacy policies?	
17.	a) What data protection training do staff (e.g. council administrator, hall bookings secretary) and councillors receive? b) What does the training involve?	
18.	a) Does anyone in the council have responsibility for reviewing personal data for relevance, accuracy and keeping it up to date? b) If so, how regularly are these activities carried out?	
19.	a) What does the council do about archiving, retention or deletion of personal data? b) How long is personal data kept before being destroyed or archived? c) Who authorises destruction and archiving?	
Part E	**MONITORING**	
20.	a) Please identify any monitoring of the following systems that takes place. 'Monitoring' includes all monitoring of systems including intercepting, blocking, recording or otherwise accessing systems whether on a full-time or occasional basis. The systems are: (i) computer networks and connections (ii) CCTV and access control systems (iii) communications systems (e.g. intercom, public address systems, radios, walkie-talkies) (iv) remote access systems (v) email and instant messaging systems (vi) telephones, voicemail, mobile phone records [Please list anything else]. b) Does the council have notices, policies or procedures relevant to this monitoring?	

Appendix 3 – Consent Form

(INSERT YOUR COUNCIL LOGO HERE)

CONSENT FORM

[Suggested introduction:]

"Your privacy is important to us and we would like to communicate with you about the council and its activities. To do so we need your consent. Please fill in your name and address and other contact information below and confirm your consent by ticking the boxes below."

		If you are aged 13 or under your parent or guardian should fill in their details below to confirm their consent
Name	.....	.....
Address	.....	.....
	.....	.....
	.....	.....
Signature	.....	.....
Date	.....	.....

Please confirm your consent below. You can grant consent to any or all of the purposes listed. You can find out more about how we use your data from our "Privacy Notice" which is available from our website or from the council Office or at [insert URL].

You can withdraw or change your consent at any time by contacting the council office.

☐ We may contact you to keep you informed about what is going on in the council's area or other local authority areas including news, events, meetings, clubs, groups and activities. These communications may also sometimes appear on our website, or in printed or electronic form (including social media).

☐ We may contact you about groups and activities you may be interested in participating in.

☐ We may use your name and photo in our newsletters, bulletins or on our website, or our social media accounts (for example our Facebook page or Twitter account).

☐ [Optional Additional Activities for councils to add if not included above.]

Keeping in touch:

☐ Yes please, I would like to receive communications by email

☐ Yes please, I would like to receive communications by telephone

☐ Yes please, I would like to receive communications by mobile phone including text message

☐ Yes please, I would like to receive communications by social media (for example Facebook, Twitter, Instagram, WhatsApp)

☐ Yes please, I would like to receive communications by post

Appendix 4 – Privacy Notices

[Please note: There are two privacy notices in this Appendix. The first is to be used for residents and members of the general public (but not for staff, councillors or anyone with a role in the local council). The second privacy notice is for staff members, councillors and anyone else with a role in the council.]

[Insert council logo here]

GENERAL PRIVACY NOTICE

Your personal data – what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual (e.g. a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify the staff in the first list then the first list will also be treated as personal data). The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the "GDPR) and other legislation relating to personal data and rights such as the Human Rights Act.

Who are we?

This Privacy Notice is provided to you by the [insert name of council] which is the data controller for your data.

Other data controllers the council works with:

- [e.g. other data controllers, such as local authorities
- Community groups
- Charities
- Other not for profit entities
- Contractors
- Credit reference agencies]

We may need to share your personal data we hold with them so that they can carry out their responsibilities to the council. If we and the other data controllers listed above are processing your data jointly for the same purposes, then the council and the other data controllers may be "joint data controllers" which mean we are all collectively responsible to you for your data. Where each of the parties listed above are processing your data for their own independent purposes then each of us will be independently responsible to you and if you have any questions, wish to exercise any of your rights (see below) or wish to raise a complaint, you should do so directly to the relevant data controller.

A description of what personal data the council processes and for what purposes is set out in this Privacy Notice.

The council will process some or all of the following personal data where necessary to perform its tasks:

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to the services provided by a council, or where you provide them to us, we may process information such as gender, age, marital status, nationality, education/work history, academic/professional qualifications, hobbies, family composition, and dependants;
- Where you pay for activities such as use of a council hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- The personal data we process may include sensitive or other special categories of personal data such as criminal convictions, racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sexual life or orientation.

How we use sensitive personal data

- We may process sensitive personal data including, as appropriate:
  - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
  - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
  - in order to comply with legal requirements and obligations to third parties.
- These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
  - In limited circumstances, with your explicit written consent.
  - Where we need to carry out our legal obligations.
  - Where it is needed in the public interest.
- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

The council will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

We use your personal data for some or all of the following purposes:

- To deliver public services including to understand your needs to provide the services that you request and to understand what we can do for you and inform you of other relevant services;
- To confirm your identity to provide some services;
- To contact you by post, email, telephone or using social media (e.g., Facebook, Twitter, WhatsApp);
- To help us to build up a picture of how we are performing;
- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions;
- To enable us to meet all legal and statutory obligations and powers including any delegated functions;
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury;
- To promote the interests of the council;
- To maintain our own accounts and records;
- To seek your views, opinions or comments;
- To notify you of changes to our facilities, services, events and staff, councillors and other role holders;

- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives;
- To process relevant financial transactions including grants and payments for goods and services supplied to the council
- To allow the statistical analysis of data so we can plan the provision of services.

Our processing may also include the use of CCTV systems for the prevention and prosecution of crime.

What is the legal basis for processing your personal data?

The council is a public authority and has certain powers and obligations. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of the council's statutory functions and powers. Sometimes when exercising these powers or duties it is necessary to process personal data of residents or people using the council's services. We will always take into account your interests and rights. This Privacy Notice sets out your rights and the council's obligations to you.

We may process personal data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the use of sports facilities, or the acceptance of an allotment garden tenancy

Sometimes the use of your personal data requires your consent. We will first obtain your consent to that use.

Sharing your personal data

This section provides information about the third parties with whom the council may share your personal data. These third parties have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. It is likely that we will need to share your data with some or all of the following (but only where necessary):

- The data controllers listed above under the heading "Other data controllers the council works with";
- Our agents, suppliers and contractors. For example, we may ask a commercial provider to publish or distribute newsletters on our behalf, or to maintain our database software;
- On occasion, other local authorities or not for profit bodies with which we are carrying out joint ventures e.g. in relation to facilities or events for the community.

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

Your rights and your personal data

You have the following rights with respect to your personal data:

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1) The right to access personal data we hold on you

- At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.
- There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2) The right to correct and update the personal data we hold on you

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3) The right to have your personal data erased

- If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.
- When we receive your request we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

4) The right to object to processing of your personal data or to restrict it to certain purposes only

- You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5) The right to data portability

- You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6) The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained

- You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7) The right to lodge a complaint with the Information Commissioner's Office.

- You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. [Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas].

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on this web page [add URL]. This Notice was last updated in February 2018.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller, [insert council details]

Email:

[Insert council logo here]

PRIVACY NOTICE

For staff*, councillors and Role Holders**

*"Staff" means employees, workers, agency staff and those retained on a temporary or permanent basis

**Includes, volunteers, contractors, agents, and other role holders within the council including former staff*and former councillors. This also includes applicants or candidates for any of these roles.

Your personal data – what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photograph, video, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual (e.g. a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify the staff in the first list then the first list will also be treated as personal data). The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the "GDPR") and other legislation relating to personal data and rights such as the Human Rights Act.

Who are we?

This Privacy Notice is provided to you by [insert name of council] which is the data controller for your data.

The council works together with:

- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies

We may need to share personal data we hold with them so that they can carry out their responsibilities to the council and our community. The organisations referred to above will sometimes be "joint data controllers". This means we are all responsible to you for how we process your data where for example two or more data controllers are working together for a joint purpose. If there is no joint purpose or collaboration then the data controllers will be independent and will be individually responsible to you.

The council will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

What data do we process?

- Names, titles, and aliases, photographs.
- Start date / leaving date

- Contact details such as telephone numbers, addresses, and email addresses.
- Where they are relevant to our legal obligations, or where you provide them to us, we may process information such as gender, age, date of birth, marital status, nationality, education/work history, academic/professional qualifications, employment details, hobbies, family composition, and dependants.
- Non-financial identifiers such as passport numbers, driving licence numbers, vehicle registration numbers, taxpayer identification numbers, staff identification numbers, tax reference codes, and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- Financial information such as National Insurance number, pay and pay records, tax code, tax and benefits contributions, expenses claimed.
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to, CCTV footage, recordings of telephone conversations, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries and insurance claims.
- Next of kin and emergency contact information
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process and referral source (e.g. agency, staff referral))
- Location of employment or workplace.
- Other staff data (not covered above) including; level, performance management information, languages and proficiency; licences/certificates, immigration status; employment status; information for disciplinary and grievance proceedings; and personal biographies.
- CCTV footage and other information obtained through electronic means such as swipecard records.
- Information about your use of our information and communications systems.

We use your personal data for some or all of the following purposes: -

Please note: We need all the categories of personal data in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing any contractual benefits to you
- Liaising with your pension provider.
- Administering the contract we have entered into with you.
- Management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Conducting grievance or disciplinary proceedings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.
- To undertake activity consistent with our statutory functions and powers including any delegated functions.

- To maintain our own accounts and records;
- To seek your views or comments;
- To process a job application;
- To administer councillors' interests
- To provide a reference.

Our processing may also include the use of CCTV systems for monitoring purposes.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal data.

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.

We may also use your personal data in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest [or for official purposes].

How we use sensitive personal data

- We may process sensitive personal data relating to staff, councillors and role holders including, as appropriate:
  - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
  - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
  - in order to comply with legal requirements and obligations to third parties.
- These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
  - In limited circumstances, with your explicit written consent.
  - Where we need to carry out our legal obligations.
  - Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our pension scheme.
  - Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- We do not need your consent if we use your sensitive personal data in accordance with our rights and obligations in the field of employment and social security law.
- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.
- You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

- We may only use personal data relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.
- Less commonly, we may use personal data relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.
- [We will only collect personal data about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.] [Where appropriate, we will collect personal data about criminal convictions as part of the recruitment process or we may be notified of such personal data directly by you in the course of you working for us.]

What is the legal basis for processing your personal data?

Some of our processing is necessary for compliance with a legal obligation.

We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract.

We will also process your data in order to assist you in fulfilling your role in the council including administrative support or if processing is necessary for compliance with a legal obligation.

Sharing your personal data

Your personal data will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or where you first give us your prior consent. It is likely that we will need to share your data with:

- Our agents, suppliers and contractors. For example, we may ask a commercial provider to manage our HR/ payroll functions , or to maintain our database software;
- Other persons or organisations operating within local community.
- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies
- Professional advisors
- Trade unions or employee representatives

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

Your responsibilities

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

Your rights in connection with personal data

You have the following rights with respect to your personal data: -

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1. ***The right to access personal data we hold on you***

- At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.
- There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2. ***The right to correct and update the personal data we hold on you***

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3. ***The right to have your personal data erased***

- If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.
- When we receive your request we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

4. ***The right to object to processing of your personal data or to restrict it to certain purposes only***

- You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5. ***The right to data portability***

- You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6. ***The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained***

- You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7. ***The right to lodge a complaint with the Information Commissioner's Office.***

- You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. [Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas].

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing, if we start to use your personal data for a purpose not mentioned in this notice.

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on this web page [add URL]. This Notice was last updated in February 2018.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller, [Add council details]

Email:

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Appendix 5 – The role of Data Protection Officers

1. What does a Data Protection Officer do?

(a) The GDPR sets out in detail the minimum responsibilities of the Data Protection Officer ("DPO") role. GDPR specifies that DPOs "should assist the controller or the processor to monitor internal compliance with this Regulation".

(b) A DPO's duties include:

(i) informing and advising the council and its staff of their obligations in the GDPR and other data protection laws;

(ii) monitoring compliance of the council, both its practices and policies, with the GDPR and other data protection laws;

(iii) raising awareness of data protection law; providing relevant training to staff and councillors;

(iv) carrying out data protection-related audits;

(v) providing advice to the council, where requested, in relation to the carrying out of data protection impact assessments ('DPIAs') and the council's wider obligations with regard to DPIAs; and

(vi) acting as a contact point for the Information Commissioner's Office.

(c) As part of these duties to monitor compliance, DPOs may, in particular:

(i) collect information to identify processing activities;

(ii) analyse and check the compliance of processing activities; and

(iii) inform, advise and issue recommendations to the controller or the processor

(d) Monitoring of compliance does not mean that it is the DPO is personally responsible where there is an instance of non-compliance. The GDPR makes it clear that it is the controller, not the DPO, who is required to 'implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.'

(e) The appointed DPO must at all times have regard to 'the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing.' This is an overarching obligation which means that the role of the DPO will vary in proportion to the risks to the rights of individuals affected by the council's processing of personal data.

(f) The DPO should 'cooperate with the supervisory authority' (in the UK, this is the Information Commissioners Office ("ICO") and 'act as a contact point for the supervisory authority on issues relating to processing, and to consult, where appropriate, with regard to any other matter'.

(g) It is the controller or the processor, not the DPO, who is required to 'maintain a record of processing operations under its responsibility' or 'maintain a record of all categories of processing activities carried out on behalf of a controller'.

2. DPOs and DPIAs

(a) A data controller (and not the DPO) is required to carry out a data protection impact assessment ('DPIA') under the GDPR in certain circumstances.

(b) The controller must 'seek advice' from the DPO when carrying out a DPIA. DPOs have the duty to 'provide advice where requested as regards the DPIA and monitor its performance'.

(c) It is recommended that controllers should seek the advice of the DPO on the following issues:

(i) Whether or not to carry out a DPIA;

(ii) What methodology to follow when carrying out a DPIA;

(iii) Whether to carry out the DPIA in-house or whether to outsource what it safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects; and

(iv) Whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR.

(d) If the controller disagrees with the advice provided by the DPO, the DPIA documentation should specifically justify in writing why the advice has not been taken into account.

3. Data controllers and processors should ensure that:

(a) The DPO is invited to participate regularly in meetings of senior and middle management. For councils, this would include meetings of full council and relevant committee meetings.

(b) The DPO's name and contact details are provided to ICO;

(c) The DPO should be available to advise/ support councillors and relevant staff on data protection issues;

(d) The DPO is present when decisions with data protection implications are taken;

(e) All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice;

(f) The opinion of the DPO must always be given due weight. In case of disagreement it is good practice to document the reasons for not following the DPO's advice;

(g) The DPO should be promptly consulted once a data breach or another incident has occurred. This is good practice since the DPO will often have been involved in implementing data protection polices such as breach reporting and it will be important for the DPO to assess whether the policies work operationally.

4. Role Checklist

☐ Raising data protection awareness within the council, and advising on GDPR compliance;

☐ Ensuring the implementation of the appropriate documentation to demonstrate GDPR compliance;

☐ Monitoring the implementation and compliance with policies, procedures and GDPR in general;

☐ Involvement in council's handling of data breaches, including assisting and advising the council with its notification to the ICO and data subjects where necessary (but it is the council which has the obligation to notify in certain circumstances not the DPO);

☐ Liaising with the ICO, the relevant councillors and staff and with the data subjects;

☐ Monitoring Data Protection Impact Assessments;

☐ Cooperating with and acting as the contact point for the ICO on issues relating to processing'

.

Appendix 6 – DPIA Assessment Checklist

A. Under the GDPR, data protection impact assessments (DPIAs) are mandatory where the processing poses a high risk to the rights and freedoms of individuals. While they can also be carried out in other situations, councils need to be able to evaluate when a DPIA is required.

B. This checklist helps you make that assessment and provides a springboard for some of the issues you will need to consider in more detail if you do need to carry out a DPIA.

1. Do you need to carry out a DPIA?

(a) What is the objective/intended outcome of the project?

(b) Is it a significant piece of work affecting how services/operations are currently provided?

(c) Who is the audience or who will be affected by the project?

(d) Will the project involve the collection of new personal data about people? e.g. new identifiers or behavioural information relating to individuals

(e) Will the project involve combining anonymised data sources in a way that may give rise to a risk that individuals could be identified?

(f) Will the project involve combining datasets originating from different processing operations or data controllers in a way which would exceed the reasonable expectations of the individuals?

(g) Is data being processed on a large scale?

(h) Will the project compel individuals to provide personal data about themselves?

(i) Will personal data about individuals be disclosed to organisations or people who have not previously had routine access to the personal data?

(j) Will personal data be transferred outside the EEA?

(k) Is personal data about individuals to be used for a purpose it is not currently used for, or in a way it is not currently used?

(l) Will personal data about children under 13 or other vulnerable persons be collected or otherwise processed?

(m) Will new technology be used which might be seen as privacy intrusive? (e.g. tracking, surveillance, observation or monitoring software, capture of image, video or audio or location)

(n) Is monitoring or tracking or profiling of individuals taking place?

(o) Is data being used for automated decision making with legal or similar significant effect?

(p) Is data being used for evaluation or scoring? (e.g. performance at work, economic situation, health, interests or behaviour)

(q) Is sensitive data being collected including:

(i) Race

(ii) Ethnic origin

(iii) Political opinions

(iv) Religious or philosophical beliefs

(v) Trade union membership

(vi) Genetic data

(vii) Biometric data (e.g. facial recognition, finger print data)

(viii) Health data

(ix) Data about sex life or sexual orientation?

(r) Will the processing itself prevent data subjects from exercising a right or using a service or contract?

(s) Is the personal data about individuals of a kind likely to raise privacy concerns or is it personal data people would consider to be particularly private or confidential?

(t) Will the project require contact to be made with individuals in ways they may find intrusive?

2. Other issues to consider when carrying out a DPIA

(a) In addition to considering the above issues in greater detail, when conducting a DPIA, you will also need to look at issues including:

(i) The lawful grounds for processing and the capture of consent where appropriate

(ii) The purposes the data will be used for, how this will be communicated to the data subjects and the lawful grounds for processing

(iii) Who the data will be disclosed to

(iv) Where the data will be hosted and its geographical journey (including how data subjects will be kept informed about this)

(v) The internal process for risk assessment

(vi) Who needs to be consulted (DPO, data subjects, the Information Commissioners Office ("ICO"))

(vii) Data minimisation (including whether data can be anonymised)

(viii) How accuracy of data will be maintained

(ix) How long the data will be retained and what the processes are for deletion of data

(x) Data storage measures

(xi) Data security measures including what is appropriate relative to risk and whether measures such as encryption or pseudonymisation can be used to reduce risk

(xii) Opportunities for data subject to exercise their rights

(xiii) What staff or, as appropriate, councillor training is being undertaken to help minimise risk

(xiv) The technical and organisational measures used to reduce risk (including allowing different levels of access to data and red flagging unusual behaviour or incidents)

3. The GDPR requires that councils carry out a DPIA when processing is likely to result in a high risk to the rights and freedoms of data subjects. For a council, examples might include using CCTV to monitor public areas.

4. If two or more of the following apply, it is likely that you will be required to carry out a DPIA. This does not apply to existing systems but would apply if you introduced a new system.

1. Profiling is in use. Example: you monitor website clicks or behaviour and record people's interests. ☐

2. Automated-decision making. Example: when processing leads to the potential exclusion of individuals. ☐

3. CCTV surveillance of public areas. Processing used to observe, monitor or control data subjects. ☐

4. Sensitive personal data as well as personal data relating to criminal convictions or offences. ☐

5. Large scale data processing. There is no definition of "large scale". However consider: the number of data subjects concerned, the volume of data and/or the range of different data items being processed. ☐

6. Linked databases - in other words, data aggregation. Example: two datasets merged together, which could "exceed the reasonable expectations of the user" e.g. you merge your mailing list with another council, club or association. ☐

7. Data concerning vulnerable data subjects, especially when power imbalances arise, e.g. staff-employer, where consent may be vague, data of children, mentally ill, asylum seekers, elderly, patients. ☐

8. "New technologies are in use". E.g. use of social media, etc. ☐

9. Data transfers outside of the EEA. ☐

10. "Unavoidable and unexpected processing". For example, processing performed on a public area that people passing by cannot avoid. Example: Wi-Fi tracking. ☐

Appendix 7 – Subject access policy and template response letters.

Subject Access Requests ("SAR") Checklist

A. Inform data subjects of their right to access data and provide an easily accessible mechanism through which such a request can be submitted (e.g. a dedicated email address).

B. Make sure a SAR policy is in place within the council and that internal procedures on handling of SARs are accurate and complied with. Include, among other elements, provisions on:

(1) Responsibilities (who, what)

(2) Timing

(3) Changes to data

(4) Handling requests for rectification, erasure or restriction of processing.

C. Ensure personal data is easily accessible at all times in order to ensure a timely response to SARs and that personal data on specific data subjects can be easily filtered.

D. Where possible, implement standards to respond to SARs, including a standard response.

1. Upon receipt of a SAR

(a) Verify whether you are controller of the data subject's personal data. If you are not a controller, but merely a processor, inform the data subject and refer them to the actual controller.

(b) Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.

(c) Verity the access request; is it sufficiently substantiated? Is it clear to the data controller what personal data is requested? If not: request additional information.

(d) Verify whether requests are unfounded or excessive (in particular because of their repetitive character); if so, you may refuse to act on the request or charge a reasonable fee.

(e) Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR.

(f) Verify whether you process the data requested. If you do not process any data, inform the data subject accordingly. At all times make sure the internal SAR policy is followed and progress can be monitored.

(g) Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.

(h) Verify whether the data requested also involves data on other data subjects and make sure this data is filtered before the requested data is supplied to the data subject; if data cannot be filtered, ensure that other data subjects have consented to the supply of their data as part of the SAR.

2. Responding to a SAR

(a) Respond to a SAR within one month after receipt of the request:

(i) If more time is needed to respond to complex requests, an extension of another two months is permissible, provided this is communicated to the data subject in a timely manner within the first month;

(ii) if the council cannot provide the information requested, it should inform the data subject on this decision without delay and at the latest within one month of receipt of the request.

(b) If a SAR is submitted in electronic form, any personal data should preferably be provided by electronic means as well.

(c) If data on the data subject is processed, make sure to include as a minimum the following information in the SAR response:

(i) the purposes of the processing;

(ii) the categories of personal data concerned;

(iii) the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules[1] or EU model clauses[2];

(iv) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;

(v) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(vi) the right to lodge a complaint with the Information Commissioners Office ("ICO");

(vii) if the data has not been collected from the data subject: the source of such data;

(viii) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(d) Provide a copy of the personal data undergoing processing.

[1] "Binding Corporate Rules" is a global data protection policy covering the international transfer pf personal data out of the European Union. It requires approval of a data protection regulator in the European Union. In most cases this will be the relevant regulator where an organisations head quarters is located. In the UK, the relevant regulator is the Information Commissioner's Office.

[2] "EU model clauses" are clauses approved by the European Union which govern the international transfer of personal data. The clauses can be between two data controllers or a data controller and a data processor.

Sample Subject Access Requests Policy

What must I do?

1. ***MUST***: On receipt of a subject access request you must **forward** it immediately to [ ]
2. ***MUST***: We must correctly **identify** whether a request has been made under the Data Protection legislation
3. ***MUST***: A member of staff, and as appropriate, councillor, who receives a request to locate and supply personal data relating to a SAR must make a full exhaustive **search** of the records to which they have access.
4. ***MUST***: All the personal data that has been requested must be **provided** unless an exemption can be applied.
5. ***MUST***: We must **respond** within one calendar month after accepting the request as valid.
6. ***MUST***: Subject Access Requests must be undertaken **free of charge** to the requestor unless the legislation permits reasonable fees to be charged.
7. ***MUST***: Councillors and managers must ensure that the staff they manage are **aware** of and follow this guidance.
8. ***MUST***: Where a requestor is not satisfied with a response to a SAR, the council must manage this as a **complaint**.

How must I do it?

1. Notify [ ] upon receipt of a request.
2. We must ensure a request has been received in writing where a data subject is asking for sufficiently well-defined personal data held by the council relating to the data subject. You should clarify with the requestor what personal data they need. They must supply their address and valid evidence to prove their identity. The council accepts the following forms of identification (* These documents must be dated in the past 12 months, +These documents must be dated in the past 3 months):
    - Current UK/EEA Passport
    - UK Photocard Driving Licence (Full or Provisional)
    - Firearms Licence / Shotgun Certificate
    - EEA National Identity Card
    - Full UK Paper Driving Licence
    - State Benefits Entitlement Document*
    - State Pension Entitlement Document*
    - HMRC Tax Credit Document*
    - Local Authority Benefit Document*
    - State/Local Authority Educational Grant Document*
    - HMRC Tax Notification Document
    - Disabled Driver's Pass
    - Financial Statement issued by bank, building society or credit card company+
    - Judiciary Document such as a Notice of Hearing, Summons or Court Order
    - Utility bill for supply of gas, electric, water or telephone landline+
    - Most recent Mortgage Statement
    - Most recent council Tax Bill/Demand or Statement
    - Tenancy Agreement
    - Building Society Passbook which shows a transaction in the last 3 months and your address
3. Depending on the degree to which personal data is organised and structured, you will need to search emails (including archived emails and those that have been deleted but are still recoverable), Word documents, spreadsheets, databases, systems, removable media (for example, memory sticks, floppy disks, CDs), tape recordings, paper records in relevant filing systems etc. which your area is responsible for or owns.

4. You must not withhold personal data because you believe it will be misunderstood; instead, you should provide an explanation with the personal data. You must provide the personal data in an "intelligible form", which includes giving an explanation of any codes, acronyms and complex terms. The personal data must be supplied in a permanent form except where the person agrees or where it is impossible or would involve undue effort. You may be able to agree with the requester that they will view the personal data on screen or inspect files on our premises. You must redact any exempt personal data from the released documents and explain why that personal data is being withheld.

5. Make this clear on forms and on the council website

6. You should do this through the use of induction, my performance and training, as well as through establishing and maintaining appropriate day to day working practices.

7. A database is maintained allowing the council to report on the volume of requests and compliance against the statutory timescale.

8. When responding to a complaint, we must advise the requestor that they may complain to the Information Commissioners Office ("ICO") if they remain unhappy with the outcome.

E. Sample letters

1. All letters must include the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules[3] or EU model clauses[4];

(d) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with the Information Commissioners Office ("ICO");

(g) if the data has not been collected from the data subject: the source of such data;

(h) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Replying to a subject access request providing the requested personal data

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

[3] "Binding Corporate Rules" is a global data protection policy covering the international transfer of personal data out of the European Union. It requires approval of a data protection regulator in the European Union. In most cases this will be the relevant regulator where an organisations head quarters is located. In the UK, the relevant regulator is the Information Commissioner's Office.

[4] "EU model clauses" are clauses approved by the European Union which govern the international transfer of personal data. The clauses can be between two data controllers or a data controller and a data processor.

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. We are pleased to enclose the personal data you requested.

Include 1(a) to (h) above.

Copyright in the personal data you have been given belongs to the council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely"

3. Release of part of the personal data, when the remainder is covered by an exemption

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. To answer your request we asked the following areas to search their records for personal data relating to you:

- [List the areas]

I am pleased to enclose *[some/most]* of the personal data you requested. *[If any personal data has been removed]* We have removed any obvious duplicate personal data that we noticed as we processed your request, as well as any personal data that is not about you. You will notice that *[if there are gaps in the document]* parts of the document(s) have been blacked out. *[OR if there are fewer documents enclose]* I have not enclosed all of the personal data you requested. This is because *[explain why it is exempt]*.

Include 1(a) to (h) above.

Copyright in the personal data you have been given belongs to the council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published, or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely"

4. Replying to a subject access request explaining why you cannot provide any of the requested personal data

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*.

I regret that we cannot provide the personal data you requested. This is because *[explanation where appropriate]*.

[Examples include where one of the exemptions under the data protection legislation applies. For example the personal data might include personal data is 'legally privileged' because it is contained within legal advice provided to the council or relevant to on-going or preparation for litigation. Other exemptions include where the personal data identifies another living individual or relates to negotiations with the data subject. Your data protection officer will be able to advise if a relevant exemption applies and if the council is going to rely on the exemption to withhold or redact the data disclosed to the individual, then in this section of the letter the council should set out the reason why some of the data has been excluded.]

Yours sincerely"

Appendix 8 – Privacy Policy Checklist

A. This checklist is designed to help draft a privacy policy. The GDPR requires certain information must be included in a Privacy Notice (see Appendix 4) but the council has more freedom about the contents of its Privacy Policy but it is recommended that you provide similar information to that included in your General Privacy Notice.

B. This checklist is designed to help you gather the information you will need to put a GDPR-compliant privacy policy on your website.

1. Council information

2. Who are the data controllers?

3. What personal data is collected?

4. With whom is the personal data shared

5. Data Subject Rights

6. Data transfers outside the EEA

7. How will changes to the policy be communicated?

8. Contact details and information to provide

Sample Policy

1. Your personal data – what is it?

"Personal data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address, or address). Identification can be by the personal data alone or in conjunction with any other personal data. The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the "GDPR) and other local legislation relating to personal data and rights such as the Human Rights Act.

2. Council information

This Privacy Policy is provided to you by [insert name of council] which is the data controller for your data.

- Is personal data collected from a website? If so what is the website address of the site that the user's personal data is collected from?
- Council address

3. Who are the data controllers?

- Are there any joint controller arrangements? (If yes, include details of the essence of this arrangement)?
- [other data controllers, such as local authorities]
- Community groups
- Charities
- Other not for profit entities
- Contractors
- Credit reference agencies

4. What personal is collected?

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to the services provided by a council, or where you provide them to us, we may process demographic information such as gender, age, , marital status, nationality, education/work histories, academic/professional qualifications, hobbies, family composition, and dependants;

- Where you pay for activities such as use of a council hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- [The data we process may include sensitive personal data or other special categories of data such as racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sex life or sexual orientation].
- Website data - Is activity information (including user behaviour data) collected? e.g.
  - Information from synching with other software or services
  - Interaction with social media (functional and/or marketing) and what information is available?
  - Information about payments
  - Access to social media profiles
  - Demographic information
- Information collected automatically from use of the service? e.g.
  - Device information (nature of device and/ or identifiers)
  - Log information (including IP address)
  - Location information (how is location collected/inferred)
  - Device sensor information
  - Site visited before arriving
  - Browser type and or OS
  - Interaction with email messages
- Information from other sources? (identify the sources) e.g.
  - Referral or recommendation programmes
  - Publicly accessible sources
- Information from cookies or similar technologies (incl. in-app codes) (including whether session or persistent) e.g.
  - Essential login/authentication or navigation
  - Functionality – remember settings
  - Performance & Analytics – user behaviour
  - Advertising/retargeting
  - Any third party software served on users
  - Other
- Nature of any outbound communications with website users
  - Email
  - Telephone (voice)
  - Telephone (text)

5. The council will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

6. We use your personal data for some or all of the following purposes:

- To deliver public services including to understand your needs to provide the services that you request and to understand what we can do for you and inform you of other relevant services;
- To confirm your identity to provide some services;
- To contact you by post, email, telephone or using social media (e.g., Facebook, Twitter, WhatsApp);
- To help us to build up a picture of how we are performing;
- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions;
- To enable us to meet all legal and statutory obligations and powers including any delegated functions;

- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury;
- To promote the interests of the council;
- To maintain our own accounts and records;
- To seek your views, opinions or comments;
- To notify you of changes to our facilities, services, events and staff, councillors and role holders;
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives;
- To process relevant financial transactions including grants and payments for goods and services supplied to the council
- To allow the statistical analysis of data so we can plan the provision of services.

Our processing may also include the use of CCTV systems for the prevention and prosecution of crime.

7. What is the legal basis for processing your personal data?

The council is a public authority and has certain powers and duties. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of the council's statutory functions and powers. Sometime when exercising these powers or duties it is necessary to process personal data of residents or people using the council's services. We will always take into account your interests and rights. This Privacy Policy sets out your rights and the council's obligations to you in detail.

We may also process personal data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the use of sports facilities, or the acceptance of an allotment garden tenancy.

Sometimes the use of your personal data requires your consent. We will first obtain your consent to that use.

8. Sharing your personal data

The council will implement appropriate security measures to protect your personal data. This section of the Privacy Policy provides information about the third parties with whom the council will share your personal data. These third parties also have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. It is likely that we will need to share your data with some or all of the following (but only where necessary):

- Our agents, suppliers and contractors. For example, we may ask a commercial provider to publish or distribute newsletters on our behalf, or to maintain our database software;
- On occasion, other local authorities or not for profit bodies with which we are carrying out joint ventures e.g. in relation to facilities or events for the community.

9. How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is current best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

10. Your rights and your personal data

You have the following rights with respect to your personal data:

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

(i) The right to access personal data we hold on you
(ii) The right to correct and update the personal data we hold on you

(iii) The right to have your personal data erased
(iv) The right to object to processing of your personal data or to restrict it to certain purposes only
(v) The right to data portability
(vi) The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained
(vii) The right to lodge a complaint with the Information Commissioner's Office.

You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

11. Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. [Our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas].

12. Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Policy, then we will provide you with a Privacy Notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

13. Changes to this policy

We keep this Privacy Policy under regular review and we will place any updates on this web page [add URL]. This Policy was last updated in February 2018.

14. Contact Details

Please contact us if you have any questions about this Privacy Policy or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller, [insert council details]
Email:

Appendix 9 – Part A: Checklist of what to include in a security incident response policy.

A. A data breach of any size is a crisis management situation, which could put an entire council at risk. Data security is not an IT issue, it is an organisational risk, and breach response should involve people from a number of roles across the council.

B. Planning for a breach is therefore essential; every council should have in place a breach response plan, and should designate, in advance, a breach response team which can be convened at short notice to deal with the crisis.

C. Understanding the issues that arise in a breach situation, and practising managing a breach, are essential to effective breach response. Failure to plan and practise increases the regulatory, litigation and reputation risk to the entire council.

D. The checklist below sets out the key issues which a council should consider in preparing for a data breach.

1. The breach response plan

(a) Do you know who should be notified within the council if there is a data breach?

(b) What happens if one of your team in (a) above is away on holiday or otherwise absent. Is there a back-up plan?

(c) Do you have clear reporting lines and decision-making responsibility?

(d) Do you understand what external assistance you might need, with providers in place in advance?

(e) Do you have designated person(s) responsible for managing breaches, with full decision making authority?

(f) Do you have processes for triaging incidents, identifying actual breaches and activating the breach response team?

(g) Is your breach response plan up to date?

(h) Have you tested your breach response plan?

2. Legal issues

(a) Do you have a process for maintaining legal privilege and confidentiality?

(b) Can you pause document destruction processes?

(c) Do you have appropriate evidence gathering capability so you can collect information about the breach?

(d) Do you know who your specialist external lawyers who can manage the investigation and give legal advice are?

(e) Do you have a process for managing and logging steps taken in the investigation?

(f) Do you understand your contractual rights and obligations with third parties?

(g) Can you quickly identify third parties you may need to notify?

(h) Do you have appropriate contractual rights to be notified of breaches by third parties?

(i) Do you know how to contact the Information Commissioners Office ("ICO") and with law enforcement who you can involve quickly if necessary?

(j) If you hold credit/ debit card data, do you need to notify your payment processor?

(k) Do you need advice on the legal options available to quickly gather evidence from third parties?

(l) Do you understand your potential liabilities to third parties?

(m) Can you gather information about the breach including taking statements from staff members or councillors who might have seen unusual activity?

(n) Do you understand when you should consider notifying data subjects and / or regulators?

3. Forensic IT

(a) Do you have access to qualified forensic IT capability, either internally or externally?

(b) Do you understand the basic IT do's and don'ts of responding to data breaches?

(c) Do you have an asset inventory to help you identify potentially compromised devices, where those devices are and in whose possession?

(d) Do you understand how data flows in your council, in practice?

(e) Can you quickly secure and isolate potentially compromised devices and data, without destroying evidence?

(f) Can you quickly ensure physical security of premises?

4. Cyber breach insurance

(a) Do you have cyber breach insurance, or other insurance which may cover a data breach?

(b) Do you understand the process for (a) notifying breaches and (b) obtaining consent for actions from insurers?

(c) Do you have emergency contact details for your brokers?

5. Data

(a) Do you know what data you hold (and what you shouldn't hold)?

(b) Is your data appropriately classified?

(c) Do you have, and apply, data destruction policies?

(d) Do you know what data is encrypted, how it is encrypted, and when it may be unencrypted on your systems?

(e) Do you have regularly check you are complying with your retention policy to ensure you are storing only the data you should be?

(f) Do you have appropriate additional protection for sensitive data?

(g) Do you have data loss prevention or similar tools?

(h) Do you understand your logs, how long you retain them for and what they can (or cannot) tell you?

(i) Do you have appropriate logging of staff/ councillor access to data?

6. Data subjects

(a) Do you understand when you should consider notifying data subjects?

(b) Do you understand the contractual and legal rights of data subjects?

(c) Can you quickly prepare appropriately worded notifications to data subjects?

(d) Do you understand the potential harm to data subjects of loss of the different types of data that you hold?

(e) Do you have the ability to appropriately triage and deal with a breach?

(f) Are councillors and staff appropriately trained as to how to deal with data subjects in a breach scenario?

7. Public Relations ("PR")

(a) Do you have access to PR capability experienced in dealing with data breaches?

(b) Do you have template pro-active and re-active press statements?

(c) Can you actively monitor social media after a breach?

Appendix 9 – Part B: Cybersecurity checklist

E. Data security is an ever-increasing risk for most organisations including councils. However, the number of breaches which are the result of highly sophisticated attacks from hackers is still very limited; most breaches are still the result of human error or relatively unsophisticated phishing attacks.

F. Many of the steps that councils can take to limit the risk and impact of a personal data breach are relatively simple to implement, but require effective policies and controls to implement. Good information security crosses over a number of policies – it is not just a matter of putting in place an information security policy. The checklist below sets out the key issues that a council should deal with, and which should be implemented where appropriate across the entire suite of internal policies.

1. Glossary

(a) **"Acceptable use policy"** or fair use policy is a set of rules applied by the owner, creator or administrator of a network, website, or service, which restrict the ways in which the network, website or system may be used and sets guidelines as to how it should be used.

(b) "**Bring Your Own Device**" ("BYOD") policy is useful where staff are permitted to use their own tablets, mobile devices and other IT equipment and deals with appropriate security measures that they should comply with.

(c) "**Cyber security**" is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

(d) **"Firewall**" is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

(e) **"Multifactor authentication"** is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction for example using a password and a separate delivered pin number (sometimes described as "2 step" authentication).

(f) **"Network security policy**" is a generic document that outlines rules for computer network access, determines how policies are enforced and lays out some of the basic architecture of the security/ network security environment.

(g) **"Penetration testing**" (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

(h) "**Red teaming**" using consults to test your physical and systems security.

(i) "**Remote access policy**" is a document which outlines and defines acceptable methods of remotely connecting to the internal network.

(j) **"Remote access"** is the ability to get access to a computer or a network from a remote distance.

(k) **"Wifi"** a facility allowing computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area.

2. Do you have appropriate policies in place?

(a) Information security policy

(b) Privacy policy

(c) "Bring Your Own Device" ("BYOD")policy

(d) Remote access policy

(e) Network security policy

(f) Acceptable use/internet access policy

(g) Email and communication policy

3. Depending on how your policies are structured, the issues below may appear in one or more of these policies.

(a) Are your policies checked and updated on a regular basis and enforced?

(b) Is there a council member with responsibility for cyber security?

(c) Do you have clear responsibility for cyber security, with clear reporting lines and decision-making authority?

(d) Do you ensure physical security of premises?

(e) Do you allocate sufficient budget to cyber security?

(f) Do you subscribe to cyber security updates so that you are aware of threats?

(g) Do you have an effective breach response plan, and do you test and update it regularly?

(h) Do you have cyber breach insurance in place?

4. People

(a) Do you have appropriate mechanisms for staff and councillors to be able to report suspicious emails quickly and effectively?

(b) Do you train staff and councillors on cyber security regularly?

(c) Do you test staff and councillors, for example by sending spoof phishing emails?

(d) Do councillors and staff undertake reviews to ensure that they understand cyber security risks, and are results checked to ensure improvement?

(e) Do you have proper processes for when staff or councillors join or leave the council, and are they applied in practice?

(f) Do staff and councillors understand the risks of using public wifi?

(g) Do you conduct appropriate checks on new staff and councillors to understand if they are a potential security risk?

5. Hardware, data, encryption and technology

(a) Is backup personal data encrypted?

(b) Do you have appropriate mechanisms for securely sending files?

(c) Do you have a list of servers, and individuals who are responsible for ensuring that they are up to date?

(d) Do you have appropriate firewalls and intrusion detection software?

(e) Are your wireless networks appropriately secured?

(f) Do you regularly check the operating systems, data and software against a 'good known state' baseline?

(g) Do you review unsuccessful attacks and probes / scans?

(h) Do you have an inventory (or list of) hardware and software you use?

(i) Do you appropriately limit access to data on a 'need to know' basis?

(j) Do you back-up personal data on a regular basis?

(k) Do you apply regular IT updates to your computer hardware and software?

(l) Do you ensure that staff and councillors have anti-virus software loaded and active on their devices at all times?

(m) Do you have appropriate policies regarding use of external hard drives or USB drives?

(n) Do you conduct regular penetration tests and / or red teaming, with appropriate analysis of results?

6. Third parties

(a) Do you properly understand risks arising from third party service providers?

(b) Do you undertake due diligence before engaging third party service providers?

(c) Do you assess third parties for cyber security or data protection risks?

(d) Do you have obligations in your contracts with third parties requiring them to take steps to keep data secure?

(e) If you use cloud storage, do you have contractual rights to be notified quickly of potential security issues?

7. Remote access/BYOD

(a) Do you require multifactor authentication where appropriate?

(b) Do you allow remote access?

(c) If so, do you have the right software and controls in place to ensure it is secure?

(d) Do you have policies to secure mobile devices?

(e) Is data encrypted on mobile devices?

(f) Can mobile devices be remotely wiped?

(g) If you use BYOD, do you apply restrictions to maintain security?

8. User accounts / passwords

(a) Do you require unique user accounts?

(b) Do you require multifactor authentication where appropriate?

(c) Do you restrict administrator accounts to the minimum necessary?

(d) Do you require strong, hard to guess, passwords?

(e) Do you automatically prevent use of common passwords?

Appendix 10 – A template of a council's internal register of processing activities

Schedule of Processing, Personal Data and Data Subjects

Description	Details
Subject matter of the processing	[This should be a high level, short description of what the processing is about i.e. its subject matter]
Duration of the processing	[Clearly set out the duration of the processing including dates]
Nature and purposes of the processing	[Please be as specific as possible, but make sure that you cover all intended purposes. The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc. The purposes will include those listed in the Privacy Notice in Appendix 4 e.g. for the purposes of performing the council's statutory obligations or delivering its services.]
Type of Personal Data	[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc.]
Categories of Data Subject	[Examples include: Staff (including volunteers, agents, and temporary workers), councillors, customers/, suppliers, members of the public, users of a particular website etc.]
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	[Describe how long the data will be retained for, how it be returned or destroyed]

Appendix 11 – Winckworth Sherwood Services

A. Winckworth Sherwood's Regulation, Data & Information team is regarded as one of the leading data protection practices in the UK. The firm advises a number of councils, charities and other not-for profit organisations as well as FTSE 100 and 250 companies on data privacy, related litigation, data monetisation, freedom of information, and branding issues.

B. Winckworth Sherwood has provided cutting edge data, information and privacy advice, and have assisted local councils, charities and other not-for-profit organisations in responding to cyber attacks (ensuring their reputation survives too). Here are some of the services Winckworth Sherwood is able to offer as part of a GDPR compliance programme:

1. Raising awareness	➢ Helping you prepare and deliver: Board / governor presentations ➢ Training FAQs
2. Data audits	➢ Data Audits / Surveys & Mapping
3. Update privacy processes / DPO appointment	➢ Reviewing & updating: ▪ Fair processing notices ▪ Website terms ▪ Privacy policies
4. Consent review	➢ Reviewing consents & whether they should be refreshed, marketing and social media
5. Contract review	➢ Supplier/third party contract review ➢ New contract terms Amending existing contracts ➢ Negotiation training for procurement teams
6. HR processes	➢ Review HR & internal policies and procedures including fair processing notices, privacy policies and contracts – avoiding reliance on consent
7. SAR & breach reporting	➢ Review subject access request processes SAR training ➢ Review how other rights will be implemented Review breach reporting processes
8. Mapping overseas data transfers	➢ Review international data transfers Consider Binding Corporate Rules ➢ Review use of model clauses
9. Security reviews	➢ Review & update security processes & policies ➢ Guidance on what to do in the first 24 hours after a breach ➢ Training on how to avoid reputation issues after a breach
10. DPIA support	➢ Conducting Data Protection Impact Assessments ➢ Assessing whether a DPIA is necessary

Discounted data protection advice rates for NALC members:

	Standard hourly rates for data protection advice	Discounted rates (plus VAT)
Partner	£450	£383
Associate	£300	£255
Solicitor	£200	£170

For further information please contact:

Toni Vitale Partner, Head of Regulation, Data and Information
020 3735 1934 **tvitale@wslaw.co.uk**