Report of the Town Clerk

General Data Protection regulations

Background

1. Members may be aware that the General Data Protection regulations become binding upon council on 25 May 2018.

What's changed?

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.
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.
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	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

	individuals, and the measures and safeguards implemented to mitigate these risks.	activities which use automated processing to evaluate, analyse or predict behaviour (e.g. tracking behaviour on a website).
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.
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).

Where are we now?

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.
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.
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. ***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.
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.
11.	***Appoint your Data Protection Officer.***

Recommendations

1. To note the update from the Town Clerk, and
2. To instruct the Town Clerk to provide an update to April Council, with suitable policies and privacy statements being provided to the Annual General meeting of Council., and
3. To instruct the Town Clerk to bring forward to April council a report on the staffing implications of the need to appoint a Data Protection Officer.