Action Plan ***approved*** ~~***– For approval***~~ ***17 May 2018*** ***– reviewed May 2019***

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.

		Hawstead PC response May 2018	***Update May 2019***
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.	***Agenda item at PC meeting July 17, Jan18, March 18*** ***Clerk training Nov 17, Jan 18, May 18; consider whole PC training*** ***Clerk appointed as data manager Jan 18; the need to appoint DPO to PC in abeyance as at May 18***	***No whole PC GDPR training undertaken to date; - is this necessary?*** ***Remind Councillors at start of new term of office of the need to limit circulation of any personal data without consent*** ***No longer any need for external data manager***
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	***Completed – circulated May 18***	***Remind (former) Councillors to destroy/return any old papers/digital material containing personal data***

	records of your processing activities. You should also record if you share data with any third parties. See *Error! Reference source not found.*~~*Error! Reference source not found.*~~***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.	***see data audit*** ***Review whether there Is any lawful basis for posting video of meeting/history recorder report containing personal data - ongoing*** ***Review new content of video/history recorder report before publication- ongoing*** ***Post disclaimer regarding archive HJ/history recorder report on website - complete***	***Very few if any recordings have been made of PC meetings during 18/19. Clerk will confirm at end of any given meeting whether there was a reference to personal data during recording, for which consent required prior to publication*** ***Disclaimer appears on website as to archive material.***
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	***Personal data to be minimised: - ongoing*** ***-Redact personal info from any doc circulated by email; - ongoing*** ***-Use dropbox rather than attaching doc to email to circulate***	***Ongoing requirements*** ***There has been no practical need to use dropbox***

Formatted: Not Highlight

Formatted: Not Highlight

Formatted Table

	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.	***any personal info/encryption – email list and consent log*** ***-Monitor effectiveness*** ***-Review content of video/HJ/history recorder report prior to posting - ongoing*** ***-Retrieve/destroy historic data (paper video and digital) from Councillors and volunteers; introduce, implement and monitor data retention policy*** ***Volunteers involved in Email list, HJ, speedwatch, emergency plan, website need to agree in writing to handling process for personal info - ongoing*** ***subject access request procedure set out in general privacy notice***	***Two separate email lists in operation;*** ***Hawstead PC list (details held by clerk; participants have consented)*** ***for circulating PC info only.*** ***Separate village list run by HCC and volunteers - separate to PC*** ***Consents in place from original partici***
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	***Revised consent form to be circulated to residents;*** ***log of consents to be maintained***	

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

	rely on pre-ticked boxes, silence or inactivity to gain consent instead people must positively opt-in. See our consent language in *Error! Reference source not found.~~Error! Reference source not found.~~**~~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 *Error! Reference source not found.~~Error! Reference source not found.~~**~~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	***Approve and publish privacy notices --complete*** ***Review operation of privacy notices May 2019*** ***Introduce Data retention policy – in privacy notice*** ***Review website. Ensure material added after 25 May 2018 does not include personal data without consent – in particular video and history recorder report- ongoing*** ***Add note to archive documentation on website that it has not yet been checked for personal information – provide information as to how any such information may be removed. - complete***	***Revised privacy notice attached***	**Formatted:** Not Highlight **Formatted:** Not Highlight **Formatted:** Not Highlight **Formatted:** Not Highlight **Formatted:** Not Highlight

	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.	***Put contract in place with village volunteers - item 8 below- who are involved with email list/ emergency plan info/speedwatch data/HJ to ensure correct handling of personal data .*** ***No CCTV*** ***Consider GDPR training for Councillors and village volunteers***	***Check current volunteers are up to date with consent forms*** ***Is further training really necessary?*** Formatted: Not Highlight
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.	***Consent form make provision for children***	
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	***Review those external data controllers/volunteers who receive data (payroll/HMRC/t Ed) and secure written contract – see data handling agreement – file maintained***	Formatted Table

	processors:		***Check website provider/email GDPR compliant – 1and1 have confirmed they are working toward this as at 16/5/18***	
	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	12.	13.

		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	***Introduce policy and undertake training***	***Policy in place***	

Formatted: Not Highlight

	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 *Error! Reference source not found.~~Error! Reference source not found.~~**~~Appendix 6 – DPIA Assessment Checklist~~**.	***n/a***	
11.	***Appoint your Data Protection Officer.*** See *Error! Reference source not found.~~Error! Reference source not found.~~**~~Appendix 5 – The role of Data Protection Officers~~***	***No longer erequired by Bill.***	