HOPTON AND COTON PARISH COUNCIL (HPC)

GENERAL DATA PROTECTION REGULATIONS (GDPR)

COMPLIANCE AUDIT MAY 2018

THE 12 STEPS RECOMMENDED BT THE INFORMATION COMMISSIONER

Which step is it?	**What does that mean?**	**Has it been done and if so, what document is being used?**	**If it HAS NOT been done, what needs to be done?**
STEP 1 AWARENESS	You should make sure that decision-makers and key people in your organisation are aware that the law is changing	**YES** **THE DATA PROTECTION ACT – A COUNCILLOR'S GUIDE SVG March 2018**	But you also need to look at HPC's current Risk Register
STEP 2 INFORMATION WHICH HPC HOLDS	You should document what personal data (PD)you hold, where it comes from and who you share it with i.e. you need to do an INFORMATION AUDIT	**YES** **SLCC SPREADSHEET**	You need a definition of what PERSONAL DATA IS – anything that, if read, would identify an individual. Once this is sorted, then you need to do an INFORMATION AUDIT which states: a) What is it? b) Where did it come from? c) Who do you share it with?
STEP 3 COMMUNICATING PROVACY INFORMATION	You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR	**YES** **SLCC TEMPLATES:** **1. Privacy Notice** **2. Email contact Privacy Notice** **3. Hirer's Privacy notice** **4. Councillor Privacy Notice**	Find some examples of Privacy Notices and put a plan in place for how and when you intend to use them. When collecting PD you have to tell people who you are and how you intend to use the information. You will also need to explain to people your LAWFUL BASIS FOR PROCESSING THE DATA, DATA RETENTION PERIODS, THEIR RIGHT TO COMPLAIN TO THE INFORMATION COMMISSIONER'S OFFICE (ICO) IF THEY THINK THERE IS A PROBLEM WITH THE WAY YOU ARE HANDLING THEIR DATA.

STEP 4 **INDIVIDUAL'S RIGHTS**	You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data / provide data electronically and in a commonly used format	**YES** **SLCC TEMPLATES:** 1. **Information correction** 2. **Information deletion** 3. **Right to object** 4. **Rights related to automated decision making and profiling** 5. **Complaints**	Check your procedures to ensure they cover all the rights individuals have. The right: • To be informed • Of access • To rectification • To erasure • To restrict processing particularly if someone has given his/her consent for you to hold this PD • To data portability • To object • Not to be subject to automated decision making including profiling. You need to explain to individuals, what their rights are. How would you react if someone asked to have their PD deleted? Who will make the decisions about deletion?
STEP 5 **SUBJECT ACCESS REQUESTS**	You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information e.g. you will have to explain your LAWFUL BASIS for processing PD in your PRIVACY NOTICE when you answer a SUBJECT ACCESS REQUEST	**YES** **SLCC TEMPLATES:** 1. **Subject access request**	You should update your procedures and plan how you will handle requests to take account of the new rules: • In most cases you will not be able to charge for complying with a request • You will have a month to comply rather than the current 40 days • You can refuse or charge for requests that are manifestly unfounded or excessive • If you refuse a request, you must tell the individual why and that they

			have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.
STEP 6 **LAWFUL BASIS FOR PROCESSING PERSONAL DATA**	You should identify the lawful basis for your processing activity in the GDPR, document it and update your Privacy Notice to explain it.	**Yes** **SLCC SPREADSHEET**	You need to know what the LAWFUL BASIS is which "allows" you to handle PD. Once identified, you should: 1. Inform individuals about the lawful basis under which you are processing PD and include it in your Privacy Notice 2. Document the lawful basis
STEP 7 **CONSENT**	You should review how you seek, record and manage consent and whether you need to make any changes	**YES** **A CONSENT FORM FROM AN OUTSIDE ORGANISATION**	Review how you seek, record and manage consent which must be: • Freely given • Specific • Informed • Unambiguous • Clear • Prominent • Opt-in • Properly documented • Easily withdrawn

STEP 8 **CHILDREN**	n/a	n/a	n/a
STEP 9 **DATA BREACHES**	You should make sure you have the right procedures in place to detect, report and investigate a PD breach	**YES** **SLCC TEMPLATE:** **1. Data security breach reporting form**	You should ensure that you have the right procedures in place to: • Detect a PD breach • Report a PD breach • Investigate a PD breach The GDPR introduces a duty on all organisations to report CERTAIN TYPES OF DATA BREACH to the ICO and in some cases, to INDIVIDUALS if, for example, it could result in: • Discrimination • Damage to reputation • Financial loss • Loss of confidentiality • Significant economic disadvantage • Significant social disadvantage
STEP 10 • **DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS**	You should familiarise yourself with the ICO's Code of Practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party and work out how and when to implement them in your organisation.	**YES** **SLCC TEMPLATES:** **1. What to think about when preparing the Privacy Impact Assessment** **2. Privacy Impact** **3. The initial screen questions to identify the need for a Privacy Impact Assessment**	PRIVACY BY DESIGN – now an express legal requirement. Data Protection Impact Assessments (PDIA's) are mandatory in certain circumstances – a DPIA is required in situations where data processing is likely to result in high risk to individuals, for example: • Where a new technology is being deployed • Where a profiling operation is likely to significantly affect individuals • Where there is processing on a large scale of the SPECIAL CATEGORIES OF DATA.