Agenda Item 9

Summary of initial Data Audit visit, carried out on 26/06/2018

GDPR DATA AUDIT

Tenterden Town Council

ICO Reg No. Z7347372

A Snapshot Image Report of 26th June 2018

Richard Newell
Director
GDPR-*info* Ltd

GDPR-info

Executive Summary

GDPR-*info* Ltd has been asked to act as virtual Data Protection Officers for Tenterden Town Council

Part of that process is to carry out a data audit to determine the levels of compliancy to the General Data Protection Regulation (GDPR) & subsequent Data Protection Act 2018 and identify areas of weakness which need addressing to provide a framework for the future.

It is apparent that Tenterden Town Council does have some significant issues in the way it handles data now, and once these concerns have been resolved, we feel that they will be working within the guidelines of the new legislation.

There is a requirement to carry out a training session with the staff and Counsellors of Tenterden Town Council. These must be documented and logged against the relevant training files.

GDPR-info

Overview

GDPR Info Ltd have been working with Phil Burgess, the Clerk of Tenterden Town Council to determine their exposure to the new rules of the GDPR. To achieve this, a data audit was carried out and an overview of the results are shown below.

A checklist was used to ensure all relevant parts of the Regulation were covered and further questioning often brought out other areas of Personal Data not originally identified.

It will be necessary for Tenterden Town Council to continue 'mapping' data they hold in a database in order that they can correctly administer the GDPR in the future – which the Clerk has been doing.

GDPR-info

Table of Contents

GDPR-info

Findings & Compliancy

The following areas were gained from the result of our interview with the Clerk to Tenterden Town Council. We have tried to separate the areas as much as possible and give our recommendations accordingly.

In each case we have tried to determine the type of data being processed and its level of sensitivity. We have also looked at whether the data is being shared with any other organisations.

On the right-hand side of each page is a small graphic which represents where we feel the Council is in terms of GDPR compliancy, Red indicates that you are performing badly whilst Green would indicate a good performance in the area.

At the bottom of each page is a box holding brief details of our findings & recommendations in that area.

Our initial 'Questionnaire' tables are a breakdown of the various subsections of the GDPR (for our guidance only) and ease of viewing & compatibility with the various sections and whether these are applicable to the Council and if there are areas which require looking at further. Denoted by a ☑ (yes) or a ☒ (no).

Questionnaire

Area	Question	Yes	No	N/A
Personal Data				
Personal data	Are you processing personal data?	✓	☐	☐
Sensitive (special) personal data	Are you processing sensitive personal data?	✓	☐	☐
Children's personal data	Is personal data of children collected and processed?	☐	☐	✓
Scope of application				
EU controller	Are you a controller?	✓	☐	☐
EU processor	Are you a processor?	✓	☐	☐
Main establishment	Where is the main EU HQ?	UK		
Non-EU controller / processor	Are any group companies located outside the EU that target/monitor EU subjects?	☐	☐	✓
	If so, has an EU representative established in one of the EU States where the data subjects are, been designated in writing (where appropriate)?	☐	☐	✓
	Is the EU representative mandated to be addressed (in addition to the controller / processor) by supervisory authorities and data subjects on processing issues?	☐	☐	✓
Joint controllers	Are there any joint data controller relationships?	☐	☐	✓
Lawful grounds for processing				
Lawful grounds for processing	Is there a lawful ground for processing the personal data for each processing operation?	✓	☐	☐
	Is there a lawful ground for processing any sensitive personal data for each processing operation?	✓	☐	☐
Consent	How is consent collected?			
	How is this consent demonstrated?			
	Can subjects withdraw their consent?	☐	☐	✓
Transparency requirements				
Notification of data subject	Is the data subject notified of processing?	✓	☐	☐
Source of personal data and information provided to data subject	Is data collected direct from the subject and is the required information given to them?	✓	☐	☐
	Is the data not collected from the subject and is the required information given to them?	☐	☐	✓
Other data protection principles and accountability				
Purpose limitation	Is personal data only used for the purposes for which it was originally collected?	✓	☐	☐
Data minimisation	Is the personal data limited to what is necessary for the purposes for which it is processed?	✓	☐	☐
Accuracy	Are policies and training in place to ensure personal data are checked and where inaccurate are rectified without delay?	☐	✓	☐
Storage limitation (retention)	Do privacy policies incorporate information on retention? Are there procedures in place for archiving and destruction of data?	☐	✓	☐
Integrity and confidentiality	Are appropriate security measures used to protect the data?	☐	✓	☐

Accountability	Can you demonstrate compliance with the data protection principles?	✓	☐	☐
Data subject rights				
Access to personal data	Is there a documented policy/procedure for handling subject access requests (SARs)?	☐	✓	☐
	Are individuals provided with a mechanism to request access to information held about them?	☐	✓	☐
	Is the data controller able to respond to SARs within one month?	☐	✓	☐
Data portability	Can data subjects get their personal data in a structured, commonly used and machine readable format?	☐	✓	☐
Erasure and rectification	Are individuals informed of their right to demand erasure or rectification of personal information held about them (where applicable)?	☐	✓	☐
	Are there controls and formal procedures in place to allow personal data to be erased or blocked?	☐	✓	☐
	Can lists and procedures manage such requests?	☐	✓	☐
Right to object	Are individuals told about their right to object to certain types of processing?	☐	✓	☐
	Are there policies to ensure rights can be effected in practice?	☐	✓	☐
Profiling and automated processing	Is profiling based on consent? (if so it this must be explicit).	☐	☐	✓
	Does any profiling use sensitive data?	☐	☐	✓
	Does any profiling involve children's data?	☐	☐	✓
Data security				
Appropriate technical and organisational security measures	Are the risks inherent in the processing formally evaluated, tested and assessed and have measures to mitigate those risks and ensure the security of the processing been implemented?	☐	✓	☐
	Is there a documented security programme that specifies the technical, administrative and physical safeguards for personal data?	☐	✓	☐
	Is there a documented process for resolving security related complaints and issues?	☐	✓	☐
	Is there a designated individual who is responsible for driving remediation plans for security gaps?	☐	☐	✓
	Are industry standard encryption algorithms and technologies employed for transferring, storing, and receiving individuals' sensitive personal information?	✓	☐	☐
	Is personal information systematically destroyed, erased, or anonymized when it is no longer legally required to be retained or to fulfil the purpose(s) for which it was collected?	✓	☐	☐
	Are steps taken to pseudonymize personal data where possible?	✓	☐	☐
	Can the availability and access to personal data be restored in a timely manner in the event of a physical or technical incident?	☐	✓	☐
Data breaches				
Breach response obligations	Does the organisation have a documented privacy and security Incident Response Plan and incident identification systems?	☐	✓	☐

	Are the plan and procedures regularly reviewed and road tested?	☐	✓	☐
	Are there procedures in place to notify DPAs and data subjects of a data breach (where applicable)?	☐	✓	☐
	Is there clear internal guidance explaining when notification is required and what information needs to be reported?	☐	✓	☐
	Are there clear procedures in place to notify the controller in the prescribed form of any data breach without undue delay after becoming aware of it?	☐	✓	☐
	Are data breaches documented?	☐	✓	☐
	Are there cooperation procedures in place between controllers, suppliers and other partners to deal with data breaches?	☐	✓	☐
	Have you considered data breach insurance cover? (not mandatory under GDPR)	☐	☐	✓
International data transfers (outside EEA)				
International data flow mapping	Is personal data transferred outside the EEA?	☐	☐	✓
	What type of personal data is transferred and does this include any sensitive personal data?			
	What is the purpose(s) of the transfer?			
	Who is the transfer to?			
	Are all transfers listed - including answers to the previous questions (e.g. the nature of the data, the purpose of the processing, from which country the data is exported and which country receives the data and who the recipient of the transfer is?)	☐	☐	✓
	Is the legal transfer adequacy mechanism for each transfer identified and listed?	☐	☐	✓
Legality of international transfers	Are specific transfers appropriately covered by an implemented adequacy mechanism or covered by an exception?	☐	☐	✓
Transparency	Are data subjects told of any intended transfers of their personal data?	☐	☐	✓
Transfers requested by overseas authorities or courts	Is there a policy for handling requests for disclosure/transfer of personal data to overseas authorities or courts? (The UK has opted out of this provision).	☐	☐	✓
Other controller obligations				
Technical and organisational measures	What privacy training programmes does the data controller provide for employees?	NONE AT PRESENT		
	Are there clear documented policies and procedures for all aspects of GDPR compliance?	☐	✓	☐
	Do you operate a regular audit review process?	☐	✓	☐
Privacy by design and default	Do policies and procedures build in a requirement to integrate compliance into processing activities?	☐	✓	☐
Data Protection Officers (DPOs)	Do you need to appoint a DPO?	✓	☐	☐
	If a DPO is not required, consider whether one should be appointed.	☐	☐	✓
	Where a DPO is appointed are escalation and reporting lines in place?	☐	☐	✓
Demonstrating compliance (record keeping)	How many employees does the company have?			

	Is sensitive personal data processed?	✓	☐	☐
	Are the legal grounds for processing personal data recorded?	✓	☐	☐
Data Protection Impact Assessments (DPIAs)	Do you have a process for identifying the need for and conducting (and documenting) DPIAs?	☐	✓	☐
	Do you undertake and record prior diligence of service providers?	☐	✓	☐
	Are all the stipulated terms included in processor contracts?	☐	✓	☐
Data processor contracts	Are there controller/processor contracts containing all the stipulated terms?	☐	✓	☐
Other processor obligations				
Contracts with controllers	Are there controller/processor contracts in place containing the stipulated terms?	☐	☐	✓
Use of sub-processors	Is there written authorisation for existing sub-processing arrangements?	☐	☐	✓
	Is there written authorisation for proposed sub-processing?	☐	☐	✓
	Has specific or general authorisation been provided?	☐	☐	✓
	If general authorisation, is there a process for informing the controller of any intended changes to processors?	☐	☐	✓
	Is the processing subject to a contract including stipulated terms?	☐	☐	✓
	Have the same obligations set out in the contract with the controller been imposed on the sub-processor?	☐	☐	✓
Demonstrating compliance (record keeping)	How many employees does the company have?	☐	☐	✓
	Is sensitive personal data processed?	☐	☐	✓
	Are the legal grounds for processing personal data recorded?	☐	☐	✓
Data Protection Officer (DPO)	Do you need to appoint a DPO?	☐	☐	✓
	If a DPO is not required, consider whether one should be appointed.	☐	☐	✓
	Where a DPO is appointed are escalation and reporting lines in place?	☐	☐	✓
Assistance to data controller	Are you able to assist the data controller in ensuring compliance under the GDPR?	☐	☐	✓

Subject Area: Councillor Details & Declarations of Interest	
Consisting of:	
Full Name:	✓
Full address:	✓
Tel No's: Home or Mobile	✓
Email address:	✓
DoB:	✓
National Insurance #.	☐
Bank Details of individuals	☐
Photo:	✓
Any other Information:	✓
Paper or Digital form	Both

Who supplied the information?	Subject
Stored Where?	Website/Cloud/Computer
Encrypted?	☐
Approx Records	16

Key Points

- Data held securely
- Signatures redacted

GDPR COMPLIANCY

Findings & Recommendations

All documents (paper & digital) are securely held (Locked cupboard)

All Councillor declarations signatures redacted prior to website transparency. (hinders identity theft)

Subject Area: Employment Records – STAFF	
Consisting of:	
Full Name:	✓
Full address:	✓
Tel No's: Home or Mobile	✓
Email address:	✓
DoB:	✓
National Insurance #.	✓
Bank Details of individuals	✓
Photo:	✓
Any other Information:	✓
Paper or Digital form	Both
Who supplied the information?	Subject
Stored Where?	Locked Cabinet
Encrypted?	☐
Approx Records	8

Key Points

Data held securely

GDPR COMPLIANCY

Findings & Recommendations

All documents (paper & digital) are securely held

Subject Area: Employment Records – Previous Staff / Councillors	
Consisting of:	
Full Name:	✓
Full address:	✓
Tel No's: Home or Mobile	✓
Email address:	✓
DoB:	✓
National Insurance #.	✓
Bank Details of individuals	☐
Photo:	☐
Any other Information:	✓
Paper or Digital form	Both

Who supplied the information?	Subject
Stored Where?	Cloud / Server
Encrypted?	☐
Approx Records	Various

Key Points

Data held securely

Data held for longer than necessary

GDPR COMPLIANCY

Findings & Recommendations

Councillors: Previous data held for invitation to civic events. We would recommend that any sensitive data held be erased and only the 'basic data' should be required for these events. (Name/Address/Email/tele)

Staff: Data held on ex-staff is held in the locked cabinet in the Clerks office. (Payroll system is cleared down of these ex-staff at year end). We strongly recommend that only the minimum of data is held for reference & HMRC purposes. Name/DOB/NI No./Address – from-to dates of employment – unless any previous grievance procedures as present or injuries during the course of employment – where terms are longer.

Recommend shredding the items in due course as the GDPR believes in data minimisation and not keeping records for longer than is legally necessary.

Subject Area: Employment Records – Payroll	
Consisting of:	
Full Name:	✓
Full address:	✓
Tel No's: Home or Mobile	✓
Email address:	✓
DoB:	✓
National Insurance #.	✓
Bank Details of individuals	✓
Photo:	☐
Any other Information:	✓
Paper or Digital form	Digital
Who supplied the information?	Subject
Stored Where?	Payroll Software
Encrypted?	☐
Approx Records	8

Key Points

▲ Sensitive data held in secure software

GDPR COMPLIANCY

Findings & Recommendations

Staff salaries are calculated via Sage Payroll Software on a PC by the Clerk. (Password protected). The software produces payslips which are printed out and placed in envelopes and passed out to staff.

Staff are paid salaries by bank transfer.

Subject Area: Minutes of Meetings & Confidential Records	
Consisting of:	
Full Name:	☐
Full address:	☐
Tel No's: Home or Mobile	☐
Email address:	☐
DoB:	☐
National Insurance #.	☐
Bank Details of individuals	☐
Photo:	☐
Any other Information:	✓
Paper or Digital form	Both

Who supplied the information?	Internal
Stored Where?	Website/Documents
Encrypted?	☐
Approx Records	n/a

Findings & Recommendations

Minutes of meeting are stored on the Council website for Transparency.

Minutes are also recorded and streamed live on the internet (Audio minutes website) – EU hosted. (France)

Any confidential paper documents used in meetings are given back to the Clerk after the meeting.

Key Points

- All data held securely
- EU hosted Audio website

GDPR COMPLIANCY

Subject Area: Correspondence / Emails with local residents	
Consisting of:	
Full Name:	✓
Full address:	✓
Tel No's: Home or Mobile	✓
Email address:	✓
DoB:	☐
National Insurance #.	☐
Bank Details of individuals	☐
Photo:	☐
Any other Information:	✓
Paper or Digital form	Both

Who supplied the information?	Subject
Stored Where?	Cloud
Encrypted?	☐
Approx Records	Various

Key Points

- Data held securely

GDPR COMPLIANCY

Findings & Recommendations

Any paper letters from residents which arrive in the Clerk's office are scanned & held digitally and only kept for the duration of the correspondence. Paper should be then shredded negating duplication.

All emails are dealt with in the same way.

Subject Area: Arrangements with Volunteers		Key Points
Consisting of:		
Full Name:	✓	Data held securely on PC's
Full address:	☐	
Tel No's: Home or Mobile	☐	
Email address:	✓	
DoB:	☐	
National Insurance #.	☐	
Bank Details of individuals	☐	
Photo:	☐	
Any other Information:	✓	
Paper or Digital form	Digital	

GDPR COMPLIANCY

Who supplied the information?	Subject
Stored Where?	Cloud/Email
Encrypted?	☐
Approx Records	Numerous

Findings & Recommendations

Volunteers who want to assist the council – their details are held on emails received & can be applied for on the form on the TTC website **(see Appendix)**

Volunteers should be made aware of the Data Protection Policies which operate within the Council. This can be done either on emails or via any paper forms which they may have to sign up for. Wording such as this below could be used.

Information Security

Tenterden Town Council cares to ensure the security of personal data. We make sure that your information is protected from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure. This is done through appropriate technical measures and relevant policies. We will only keep your data for the purpose it was collected for and only for as long as is necessary. After which it will be deleted. (Please view our Privacy Notice & Retention Notice online at: www.tenterdentowncouncil.gov.uk for further information)

Subject Area: Users of Hall Facilities / Hire Rooms etc.	
Consisting of:	
Full Name:	✓
Full address:	✓
Tel No's: Home or Mobile	✓
Email address:	✓
DoB:	☐
National Insurance #.	☐
Bank Details of individuals	✓
Photo:	☐
Any other Information:	✓
Paper or Digital form	Both
Who supplied the information?	Subject
Stored Where?	Paper files
Encrypted?	☐
Approx Records	Numerous

Key Points

- No Data Protection Wording on any forms
- No secure storage

GDPR COMPLIANCY

Findings & Recommendations

Booking the various rooms can be done through a general enquiry on the TTC website and 'clicking' on the particular venue & completing details which are automatically emailed to the Deputy Clerks PC (below) or by calling in and requesting an application form from the Clerk's Office.

Mayors Parlour, Assembly Room, Tenterden Recreation Ground, Football Pitch, Pavilion, St Michaels Recreation Ground, Councillor's Room

The hirer pays a deposit (variable) and completes an agreement form to hire the rooms. (Hirers bank details are taken) & personal details are entered onto a database (Rialtas-RBS Software). Once the venue has been used by the hirer the deposit is paid back to them via bank transfer. All documents relating the whole transactions (including sensitive data) are held in paper files in an open bookcase in the Deputy Clerks office. Manual Invoices are set up and sent to the hirers as MS Word Documents – Duplication of what is already on the database – it should be possible to utilise the RBS Software to work properly.

We would strongly recommend that all the above 'Supplier' files be locked in a cabinet when not in use

There is NO Data Protection Wording on any of the hirers application forms – wording such as previously mentioned in the 'Volunteer' section could be used.

Subject Area: Allotments	
Consisting of:	
Full Name:	✓
Full address:	✓
Tel No's: Home or Mobile	✓
Email address:	✓
DoB:	☐
National Insurance #.	☐
Bank Details of individuals	☐
Photo:	☐
Any other Information:	✓
Paper or Digital form	Both
Who supplied the information?	Subject
Stored Where?	Paper / Spreadsheet
Encrypted?	☐
Approx Records	Various

Key Points

- Data held on Cloud
- No Agreement (Joint Controller) in place
- Duplication of Data

GDPR COMPLIANCY

Findings & Recommendations

The TTC allotments are 'managed' by the William Judge Trust who deal directly with the 'Allotment tenant' who signs an agreement with them. (There is an acceptable Data Protection paragraph in the 'agreement' stating that the data held by them will only be used for the purpose of managing the allotment. (this must be adhered to by the Trust as any other usage of the data, such as for marketing purposes would be illegal). When a resident wants to 'own' an allotment they approach TTC and their basic details are entered onto a Allotment Waiting List Spreadsheet and held on the Cloud Drive of TTC. When an allotment becomes available, the Trust informs TTC who allocates the next resident on the waiting list & who pays the fee for renting the allotment to TTC.

Under the GDPR (Article: 26) (See Appendix) both TTC and the Trust are 'Joint Controllers' of the data and there should be an AGREEMENT (not contract) in place to show this which should be drawn up *"...reflecting the respective roles and relationships of the joint controllers vis-à-vis the data subjects. [2]The essence of the arrangement shall be made available to the data subject."*

It was also noted that whilst auditing the Admin Assistants PC there were previous Allotment Spreadsheets to view from 2011,2012 & 2013 – these should either be deleted or amalgamated into a single data source with the current Allotment Waiting list Spreadsheet and be held securely!

Subject Area: Contracts with External Companies		
Consisting of:		
Full Name:		✓
Full address:		✓
Tel No's: Home or Mobile		☐
Email address:		☐
DoB:		☐
National Insurance #.		☐
Bank Details of individuals		☐
Photo:		☐
Any other Information:		✓
Paper or Digital form		Both
Who supplied the information?		3rd Party
Stored Where?	N/A	
Encrypted?		☐
Approx Records	N/A	

Key Points

- Data held securely on suppliers
- No third-party agreements in place

GDPR COMPLIANCY

Findings & Recommendations

IT supplier – Kent IT

Website Design – WebBox (Cardiff)

CCTV Company

No third-party agreements in place with any of the above contractors – a requirement of the GDPR!

Subject Area: Electoral Roll	
Consisting of:	
Full Name:	✓
Full address:	✓
Tel No's: Home or Mobile	☐
Email address:	☐
DoB:	☐
National Insurance #.	☐
Bank Details of individuals	☐
Photo:	☐
Any other Information:	✓
Paper or Digital form	Both

Who supplied the information?	Internal
Stored Where?	Email & Safe
Encrypted?	✓
Approx Records	Numerous

Key Points

- Data held securely

GDPR COMPLIANCY

Findings & Recommendations

The paper version of the Electoral Roll is kept in a locked safe and the digital one can only be accessed with a password on a PC.

Subject Area: FOI's, Emergency Plan & Local Planning	
Consisting of:	
Full Name:	✓
Full address:	✓
Tel No's: Home or Mobile	☐
Email address:	☐
DoB:	☐
National Insurance #.	☐
Bank Details of individuals	☐
Photo:	☐
Any other Information:	✓
Paper or Digital form	Both

Who supplied the information?	Subject
Stored Where?	Paper & Digital
Encrypted?	☐
Approx Records	Various

Key Points

Data held securely

Records require updating

GDPR COMPLIANCY

Findings & Recommendations

Any Freedom of information requests which might appear in the future should be held securely & should have a retention date applied to them and this should be stated in the Councils Data Retention Policy.

Local Planning Applications can be viewed on Ashford Borough Councils website portal. Current applications for decisions by the Council are printed out for the Council meetings. Once dealt with, are destroyed.

The Council has a list of individuals for contacting in an Emergency Plan – the Clerk advised that this requires updating. (GDPR requires organisations to keep *up to date* personal information)

The individuals would be required to know about the Data Protection Policy of the Council and we would recommend that the wording used for the 'Volunteer' form previously could be also used for these individuals too.

Subject Area: Notices & Council Data Protection Policies	
Consisting of:	
Full Name:	☐
Full address:	☐
Tel No's: Home or Mobile	☐
Email address:	✓
DoB:	☐
National Insurance #.	☐
Bank Details of individuals	☐
Photo:	☐
Any other Information:	✓
Paper or Digital form	Digital

Who supplied the information?	3rd Party
Stored Where?	PC
Encrypted?	☐
Approx Records	N/A

Key Points

▼ No Policies Available

GDPR COMPLIANCY

Findings & Recommendations

Mini-newsletters: Emailed currently to 12 recipients for resident who signed up. Emailed twice yearly.

Policies: No Data Protection Polices were available. **GDPR-info will supply all required.**

Subject Area: Website	
Consisting of:	
Full Name:	☐
Full address:	☐
Tel No's: Home or Mobile	☐
Email address:	☐
DoB:	☐
National Insurance #.	☐
Bank Details of individuals	☐
Photo:	☐
Any other Information:	✓
Paper or Digital form	Digital
Who supplied the information?	3rd Party
Stored Where?	Website
Encrypted?	✓
Approx Records	N/A

Key Points

- EU Hosted
- Cookie policy in place
- No Privacy Notice

GDPR COMPLIANCY

Findings & Recommendations

Website supplied & hosted by WebBox a company based in Cardiff.

The website is hosted in the EU. (Germany)

SSL Encryption is in place

Cookie Policy is in place

No Privacy Notice!

Twitter & Facebook links managed by the Town Council

Several links to outside sites: If 'independent' it should be stated on the page that TTC are not responsible to external information.

Subject Area: Shredding		
Consisting of:		
Full Name:		☐
Full address:		☐
Tel No's: Home or Mobile		☐
Email address:		☐
DoB:		☐
National Insurance #.		☐
Bank Details of individuals		☐
Photo:		☐
Any other Information:		✓
Paper or Digital form		Paper
Who supplied the information?		Internal
Stored Where?	N/A	
Encrypted?		☐
Approx Records	N/A	

Key Points

Date securely disposed of

GDPR COMPLIANCY

Findings & Recommendations

Shredding and disposal of paper is done internally in the Clerk's Office.

Should there be larger amounts of shredding to do in the future the Council uses a company called **EDM Solutions** – who provide a **'destruction certificate'**.

Should the paper waste be 'yearly' based, and an external company used, then a data destruction spreadsheet should be set up and the information stated on it state what has been disposed of and for a set time (e.g. Paper destruction of correspondence/finance documents (2009-2010) etc. & the Data Destruction Certificate Number be added to it. *This helps if a Subject Access Request requires information from the year in question (2009-2010) and the Council can state that the information has been securely destroyed and would be no longer available for that request*

Subject Area: CCTV	
Consisting of:	
Full Name:	☐
Full address:	☐
Tel No's: Home or Mobile	☐
Email address:	☐
DoB:	☐
National Insurance #.	☐
Bank Details of individuals	☐
Photo:	✓
Any other Information:	✓
Paper or Digital form	Digital

Who supplied the information?	Internal
Stored Where?	Hard Drive Storage
Encrypted?	✓
Approx Records	N/A

Key Points

- Data stored securely
- No CCTV Policy in place

GDPR COMPLIANCY

Findings & Recommendations

The Council uses a CCTV system around the Town

There is a 14 day overwrite system

The recording system is locked in a cabinet

Staff only have access to it

The system has a battery backup.

The Council is required to add CCTV to their ICO registration and also to have a CCTV policy in place stating the above facts – **GDPR-Info Ltd to supply.**

Subject Area: Data backups and Computers	
Consisting of:	
Full Name:	☐
Full address:	☐
Tel No's: Home or Mobile	☐
Email address:	☐
DoB:	☐
National Insurance #.	☐
Bank Details of individuals	☐
Photo:	☐
Any other Information:	☐
Paper or Digital form	Select.
Who supplied the information?	Select
Stored Where?	Click here to enter text.
Encrypted?	☐
Approx Records	Click here to enter text.

Key Points

- Secure Backup Run
- Passwords not in use
- Encryption not switched on

GDPR COMPLIANCY

Findings & Recommendations

The Council run a real-time cloud backup facility for all its computers through a 'Microsoft Cloud Server'. (UK Based).

All PC's are backed up hourly

No PC's are password protected – this is a **major failure in data security** – Recommend that password access be set up and also a change password policy also be set up for a 3-6 month change.

All PC's are running Windows 10 Pro Operating system with the BitLocker Encryption system built in – The encryption is not currently switched on! (no security)

We recommend that the Clerk contacts their IT supplier to find out why they aren't switched on?

Some USB drives have been used in the past – we recommend that these be erased

Subject Area: Councillor Emails & Electronic Devices	
Consisting of:	
Full Name:	☐
Full address:	☐
Tel No's: Home or Mobile	☐
Email address:	☐
DoB:	☐
National Insurance #.	☐
Bank Details of individuals	☐
Photo:	☐
Any other Information:	✓
Paper or Digital form	Digital

Who supplied the information?		Subject
Stored Where?	N/A	
Encrypted?		✓
Approx Records	N/A	

Key Points

- TTC Domain based emails used
- Some 'personal' email addresses shown on the site through the email links

GDPR COMPLIANCY

Findings & Recommendations

Councillors use their allocated Tenterden Town Council **dot gov** email addresses when dealing with Town Council business

However, some Councillors who are also Borough Councillors through the TTC website also show other personal email addresses:

- mikebennettkm@tiscali.co.uk
- paul.clokie1@btopenworld.com
- callum@tenterden.co.uk

We would recommend that the above Councillors as they are on the TTC website should use their TTC email addresses as all the above can be 'forged' and are not safe or provide a professional image on a Council website

BYOD (Bring your own device) Councillors who use digital tablets and laptops at Council meetings should be aware of the risks involved (no Council personal identifiable data should be kept on them unless they are password protected & encrypted). **See the ICO website for further information**

Subject Area: Photocopier		Key Points
Consisting of:		
Full Name:	☐	
Full address:	☐	
Tel No's: Home or Mobile	☐	
Email address:	☐	
DoB:	☐	
National Insurance #.	☐	
Bank Details of individuals	☐	
Photo:	✓	
Any other Information:	✓	
Paper or Digital form	Digital	
Who supplied the information?	Unknown	
Stored Where?	Hard Drive	
Encrypted?	☐	
Approx Records	N/A	

GDPR COMPLIANCY

Findings & Recommendations

The Council office has the use of a photocopier. The copier has an integral hard drive – the council should be aware that the machine has the ability to store all documents which have been copied and retain them. It may be possible for an engineer to reproduce documents on the hard drive which have been previously copied. TTC must find out from the supplier as to what the suppliers' terms of hard drive retention/destruction are should the machine be changed as personal information could be stored on the internal hard drive.

Policies

Policy Area	Already in Place
Data Breach Policy	☐
Staff Privacy Policy for the staff handbook	☐
Web Privacy Notice	☐
Retention of Records	☐
Complaints Procedure	☐
Training Policy	☐
Subject Access Request Notice	☐

Policies can only be decided by the individual authority. Whilst GDPR-info Ltd can advise on content and layout, the final decision is yours.

Bear in mind that the policy needs to be even handed but ensure that the Data Subject still gets their full rights under GDPR.

Training Requirements

GDPR requires that all members of staff who come into contact with personal data are trained in the fundamentals of data protection under the Regulation.

Whilst GDPR-*info* will provide the initial training, it is the responsibility of the local authority to continue this as required, in particular training on GDPR must be added to induction training programs for both functionaries and new Members.

A complete record of all training must be held against each person in the training file, if available or against the individual's employment record.

Administration of GDPR

Introduction

There is a major requirement in GDPR to document everything done with personal data. This includes understanding where the data resides, what is held in the data, the sensitivity of data and the movement of data within and without the company.

One of the first things that will be checked by the ICO office if they carry out an inspection is the level of administration a company is carrying out with regard to its collection, storage and processing of personal data.

In the event of a data breach, again it is this administrative data which will allow Tenterden Town Council to identify the type of data breached, its level of sensitivity and who the breach may have affected. Since companies only have 72 hours after identifying a breach in which to provide the relevant information to the ICO, it makes sense to have this information readily available rather than having to assemble it from scratch at the time.

It must also be remembered that auditing the data, its use and sensitivity is not a one-off job but one which needs to be carried out on a regular basis.

The areas of GDPR that need to be administered are,

- Data Audit
  - What data is held where, types of data, sensitivity etc. Must also show the reasons for holding the data and when the data should be removed. This will be one of the company policies

- Data Transfers - A record of all data transfers for data processing. It must contain:
  - Data Source
  - Type of data
  - Name and address of Processor
  - Schedule of transfers (weekly, monthly etc.)

- Subject Access Requests – Keep a record of
  - Right to Object
  - Right to Restrict Processing

- Right to Erasure
- Right to Be Informed

- Data Breaches
  - What happened
  - When it happened
  - What Data was accessed
  - Whether data breach is serious enough to warrant informing data subjects.

- Record of DPIAs
  - a description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
  - an assessment of the necessity and proportionality of the processing in relation to the purpose.
  - an assessment of the risks to individuals.
  - The measures in place to address risk, including security and to demonstrate that you comply.
  - A DPIA can address more than one project.

- Council Policies - These include:
  - name and details of your organisation (and where applicable, of other controllers,
  - your representative and data protection officer);
  - purposes of the processing;
  - description of the categories of individuals and categories of personal data;
  - categories of recipients of personal data;
  - details of transfers to third countries including documentation of the transfer mechanism safeguards in place;
  - retention schedules; and
  - a description of technical and organisational security measures.

Appendix

The following section contains the supporting information that we have based our report on. It will allow you to look in more detail at our findings that are given earlier in this report.

Data Audit Form	**Date of Audit: 26th June 2018**
Type of Data	Personal non-sensitive/sensitive
Description of data	Various word documents / spreadsheets – paper HR files Sage Payroll Software Password protected
Employee responsible	Clerk
Date of consent to hold data	n/a
Where the data is stored	ttc.kentint.net (Y) drive
Source of the data	Council business
Purpose of the data	Council business
How the data is protected in its storage	Windows 10 Pro (Bitlocker Encryption not switched on), Windows Defender Anti-virus Paper HR files in locked cabinet
Usage restrictions	Clerk
Usage rights	Clerk
Usage frequency	Daily
Retention period	Depends on Data
Comments	**Recycle Bin** 156 items – require deleting – **NO PASSWORD IN PLACE**

Data Audit Form	**Date of Audit: 26th June 2018**
Type of Data	Personal non-sensitive/sensitive
Description of data	Various word documents / spreadsheets
Employee responsible	Accounts
Date of consent to hold data	n/a
Where the data is stored	ttc.kentint.net (Y) drive
Source of the data	Council business
Purpose of the data	Council business
How the data is protected in its storage	Windows 10 Pro (Bitlocker Encryption not switched on), Windows Defender Anti-virus
Usage restrictions	Accounts
Usage rights	Accounts
Usage frequency	Daily
Retention period	Depends on Data
Comments	**Recycle Bin** 22 items – require deleting **NO PASSWORD IN PLACE**

Data Audit Form	**Date of Audit: 26th June 2018**
Type of Data	Personal non-sensitive/sensitive
Description of data	Various word documents / spreadsheets
Employee responsible	Deputy Clerk
Date of consent to hold data	n/a
Where the data is stored	ttc.kentint.net (Y) drive
Source of the data	Council business
Purpose of the data	Council business
How the data is protected in its storage	Windows 10 Pro (Bitlocker Encryption not switched on), Windows Defender Anti-virus
Usage restrictions	Deputy Clerk
Usage rights	Deputy Clerk
Usage frequency	Daily
Retention period	Depends on Data
Comments	**Recycle Bin** 1 item – require deleting. **NO PASSWORD IN PLACE**

Data Audit Form	**Date of Audit: 26th June 2018**
Type of Data	Personal non-sensitive/sensitive
Description of data	Various word documents / spreadsheets
Employee responsible	Admin Assistant
Date of consent to hold data	n/a
Where the data is stored	ttc.kentint.net (Y) drive
Source of the data	Council business
Purpose of the data	Council business
How the data is protected in its storage	Windows 10 Pro (Bitlocker Encryption not switched on), Windows Defender Anti-virus
Usage restrictions	Admin Assistant
Usage rights	Admin Assistant
Usage frequency	Daily
Retention period	Depends on Data
Comments	**Recycle Bin** 8 items – require deleting. **NO PASSWORD IN PLACE** Cloud Drive available?? – Large amounts of information held: Allotment Waiting Lists 2011,2012,2013 containing personal sensitive information & Invoices & Deputy Clerks Signature on the Desktop as a JPG Image – all these items should be hived off and held securely OR deleted! (No reason to keep outdated documents!)

Data Audit Form	**Date of Audit: 26th June 2018**
Type of Data	Personal non-sensitive/sensitive
Description of data	Various word documents / spreadsheets
Employee responsible	TTC Laptop
Date of consent to hold data	n/a
Where the data is stored	ttc.kentint.net (Y) drive
Source of the data	Council business
Purpose of the data	Council business
How the data is protected in its storage	Windows 10 Home – **No Encryption!** Windows Defender Anti-virus
Usage restrictions	TTC Laptop
Usage rights	TTC Laptop
Usage frequency	Daily
Retention period	Depends on Data
Comments	**Recycle Bin** 9 items – require deleting. **NO PASSWORD IN PLACE** Some recordings (presumably Council meetings) – these should be deleted once uploaded to website.

Password Protection / Encryption

Understanding the difference

There is often considerable confusion between password protection and encryption. Both methods provide a level of protection, but having data encrypted means that should a machine be stolen, there would be no requirement to report a Data Breach to the ICO.

The difference between the two is possibly best described by making a couple of analogies.

Imagine a chest and on the front of the chest is a big padlock with a combination on it. People can't get past the padlock because it has a password on it (combination)

However, unbeknown to the owner of the chest there is a small hole at the bottom of the chest which is just big enough for someone to go fishing around inside and pull out whatever they want. And that is how the standard hacking events take place.

On the other hand, think of a paper shredder. In this instance all the data is chopped up into little pieces and looks a bit like small bits of confetti. The chances of knowing how to put it together are ridiculously small. And that's what happens with encryption. When the machine is closed down, the computer effectively shreds all its data. Anyone accessing the contents of the shredder would just find insignificant pieces all over the place. However, once the encryption key is entered (and this can either be a secondary password or in the case of more modern computers a special security chip) the data combines together and is read as it would be normally.

If a company has a lot of sensitive data we would insist on data encryption of the whole disk, however this is not normally the case.

Encryption of mobile computing devices.

However, any mobile devices must be encrypted in case of loss.

Mobile telephones come with this built in as do all Apple products. The biggest problems relate to USB hard drives, USB data sticks and laptop PCs.

Most USB hard drives come with encryption software which can be activated at any time. Normally this software will give the user three opportunities to login successfully before securely wiping the drive or, in some cases destroying it. USB sticks will, if chosen correctly (and normally only costing a few pounds more than basic models) will also have the same software – but this is normally destroy only. With Laptop PCs, depending on the age and power of the machine it may well be possible to download Microsoft BitLocker for free from Microsoft.com. Installation is relatively easy but does incur and extra step in logging in to the device.

Benefits of encryption

The benefits are

- Peace of mind that the data is safe from prying eyes.
- Any mobile device that is lost, whatever data it holds, will not be classed as a Data Breach if it is encrypted.

VPN – Virtual Private Network

Have you ever heard of a sniffer? This is a computer program that is used to decode data to make it readable, but in nefarious ways. The bad guys use sniffers to spy, steal data, hijack devices, and even steal identities. Sniffers are also used by the good guys to determine how secure a network is. Unencrypted data is very vulnerable to sniffers, as is any info that comes through your browser that isn't secure. Wireless connections are also particularly vulnerable to sniffers. Fortunately, you can use a virtual private network, or VPN, to protect yourself.

What Is a VPN?

A virtual private network, or VPN, is a network that allows you to communicate over a public, unsecured, unencrypted network in a private way. Most VPN tools have specific versions of encryption to secure your data. For instance, you might work from home, but you still need to send information to your office. Your business network might be very secure, but your home network might not be. However, you can use a VPN to protect yourself. Another example of a VPN is a remote access version.

With this, you can take it on the road. And, on the road, when you use the internet on a computer or other device on a public network that is not protected, your information is very vulnerable to sniffers. People use these in places that offer free Wi-Fi such as airports, hotels, and coffee shops.

This form of VPN helps to protect the data sent between your laptop or mobile device to an internet gateway. Essentially, a VPN makes a type of tunnel that prevents hackers, snoopers, and ISPs from looking at your instant messages, browsing history, credit card information, downloads, or anything that you send over a network.

What Does a VPN Do?

Security: A VPN encrypts the entire web session of the user. It makes every website just as secure as a bank or other financial site.

Bandwidth Compress: A VPN compresses all of the traffic on the server before sending it to you. This allows you to have more access to your data.

Access: There are lots of restrictions online imposed by various companies about where and when you can use their services. Further, many oppressive

governments restrict information that would lead to "free thinking". A VPN allows users to have uncensored, secure access to anything on the internet.

Privacy: A VPN masks the addresses of users and protects a person's identity from tracking.

Why Is a VPN So Important?

Your personal information is out there, and people want it. However, you certainly don't want this info to get into the wrong hands. No matter where you use your device, you are at risk of an infection or a data breach. Any unprotected internet connection is dangerous, but if you use a VPN, your transmissions are protected.

Do You Really Need a VPN?

You might wonder if you really need a VPN. Well, what you should really be asking is if you want to go out into the wild web without protection. Basically, if you do this, anyone within about 500 feet, and as little as 300 feet, in some cases, can get all of your data...if, of course, they have the right knowledge and tools. What can they see? Everything to your comments on a local news article to your bank account number and password.

If you are questioning if you need a VPN or not, you probably think that you have nothing to hide or that you have no information that a hacker would want. However, if you are online, someone wants your info. This might be as simple as an advertiser watching what sites you are visiting so they can send targeted ads. Or, it might be much more sinister.

So, should you VPN or not? It's a good idea when you are on any mobile device, including phones and tablets. You should also use a VPN if connecting to a public internet connection, such as at a hotel. Do you need it in your home? Maybe not, so you might want to use it on a case by case basis. VPNs are pretty cheap, if not free, so it might be a good investment.

The Difference Between a Proxy and a VPN

You might have also heard of a proxy. It's similar to a VPN but not quite the same.

A VPN is a virtual network that allows you to privately communicate over a network that is otherwise public. As you know, these networks protect your data between devices, including PC's, Macs Androids, iPhones, laptops, and iPads, and an internet gateway. The network does this by crafting a secure tunnel that is impenetrable. This keeps hackers, snoopers, and any ISP from viewing your activity. This includes web-browsing, downloading, instant messages, and anything else that you might send over a particular network.

A proxy server, on the other hand, is a bit different. If you use a proxy, your internet activity is anonymous. There are different ways that this works. For one, the destination server, which is the server that accepts a certain web request, gets these requests from the proxy server. This keeps you anonymous. Without a proxy server, you are no longer anonymous.

GDPR-info

Both proxies and VPNs are designed to change a person's IP address. They also manipulate your browsing practices. However, keep in mind that a proxy doesn't encrypt your connection. This means that the information that you are sending and receiving on the network could be stolen or intercepted if you are on a public Wi-Fi connection. A VPN, however, not only acts just like a proxy, but it also encrypts your information.

VPNs

- A VPN encrypts, or scrambles, data so that a hacker cannot tell what a person is doing online. In other words, a VPN offers a type of tunnel, which is where the data goes. This tunnel cannot be penetrated, and your transmissions cannot be viewed.
- A VPN is private, and it can make any public network private for those who use them. A VPN can be used on a desktop or any mobile device including laptops, phones, and tablets.
- A VPN protects data. This data includes instant messages, e-mail communications, downloads, login information, and which sites you visit.

- A VPN alters your IP address, too. This makes it seem like you are using your computer elsewhere. This makes it possible to access sites like Facebook if they are otherwise blocked.

Proxy Server

- A proxy server makes sure the user can browse with anonymity. This means the site you visit would not be able to identify anything about you. This includes your location. This comes in handy if you are somewhere that bans certain sites, such as social media.
- With a proxy server, your transmissions and data are not hidden nor encrypted. So, it can still be seen, but the server doesn't know who is behind the actions. This also means that hackers can still access information if they can get to it, such as on a public Wi-Fi connection.

Many people use a VPN with a proxy server as it gives the user the best of both worlds. You are safe, and you are anonymous. However, even when you do this, there is something to be said about being cautious when on a public Wi-Fi connection. A good rule of thumb is to only access websites that don't require any personal or sensitive information when on a public Wi-Fi connection. Here are some more do's and don'ts for when you are connected to public Wi-Fi:

Public Wi-Fi Don'ts

- Never leave your device alone when connected to public Wi-Fi — not even for a minute, such as going to a rest room. You might come back to see your laptop still there, but you also might have something a bit extra like a keylogger. This is used to capture keystrokes.
- Don't e-mail anything that is of sensitive nature. Save these e-mails for when you are on a secure network.

- Take a look at the networks before connecting to them. Make sure you are connecting to the right network and not to a network that is specifically set up to collect information, it might say "free Wi-Fi".

- Do not turn on file sharing when connected to public Wi-Fi.
- If you don't need to connect to a wireless connection, don't leave your Wi-Fi on.
- Never do any online banking or work with sensitive information when connected to these networks.
- Do not let anyone see your screen.

Public Wi-Fi Do's

- Look at your surroundings before settling into a spot for browsing.
- Make sure you sit so that your back is to a wall.
- Assume any Wi-Fi link is suspicious. Any link can be set up by a hacker, so exercise caution. Try to confirm any link by looking at the address closely.
- Ask an employee to confirm the name of the network. Hackers are clever. If you are at Joe's Coffee Shop and see two networks, JoescoffeeWifi and JoescoffeshopWifi, which one do you connect to?
- Only visit sites that you don't have to enter any personal information into. Save the others for a secure network.

After all is said and done, it's probably in your best interest to use a VPN. Hackers cannot get into these networks, nor do they have any access to them. When you choose a VPN, your data, browsing habits, and personal information is safe. All of the information you send remains encrypted, so you don't have to worry about doing your banking or accessing any sensitive information. You can also download sensitive information and send sensitive e-mails. Just make sure that there are no wandering eyes that are looking at your screen.

Otherwise, you still might put yourself at risk of snoops or thieves accessing your information.

Subject Area: Volunteer Form from Website

TENTERDEN COMMUNITY RESPONSE TEAM

I/we volunteer to join the community response team:		*(please tick box)*	
I/we would like to volunteer to be community liaison for:		*(road or street)*	
Name(s):			
Address:			
'Phone:		Email:	
Organisation (if applicable):			

Please list any relevant skills, equipment or resources you *(or your organisation)* have/has:

(continue overleaf if necessary)

Signed declaration - Each person named above must sign the declaration below.

I give my consent for the above details to be made available to those responding to an emergency affecting our community. I understand that, in accordance with the Data Protection Act (1998), the information will be handled in the strictest confidence and will only be used in an emergency situation.

Signatures			
Print Name			
Date			

Subject Area: GDPR Article 26 – Joint Controllers Agreement

Art. 26 GDPR

Enter search term here ...

Y ISSUES

1. [1] Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. [2] They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. [3] The arrangement may designate a contact point for data subjects.

2. [1] The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. [2] The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Suitable Recitals

(79) Allocation of the responsibilities

Subject Area: TTC – Hirers Application Forms

TENTERDEN TOWN COUNCIL

TENTERDEN TOWN HALL

Please complete this form and return it to the Town Clerk's office.
All information will be stored securely and treated as confidential.

Which room do you wish to book? MAYOR'S PARLOUR / ASSEMBLY ROOM

Number of guests

Day of week

Date D D M M Y Y Y Y

Time am pm

Person 1 details

Title Forename(s)

Surname

Name you would like to be called during the ceremony

Postal Address

Post Code

Home Telephone Mobile Telephone

Email Address

Which country issued / would issue your passport

Person 2 details

Title Forename(s)

Surname

Name you would like to be called during the ceremony

Postal Address

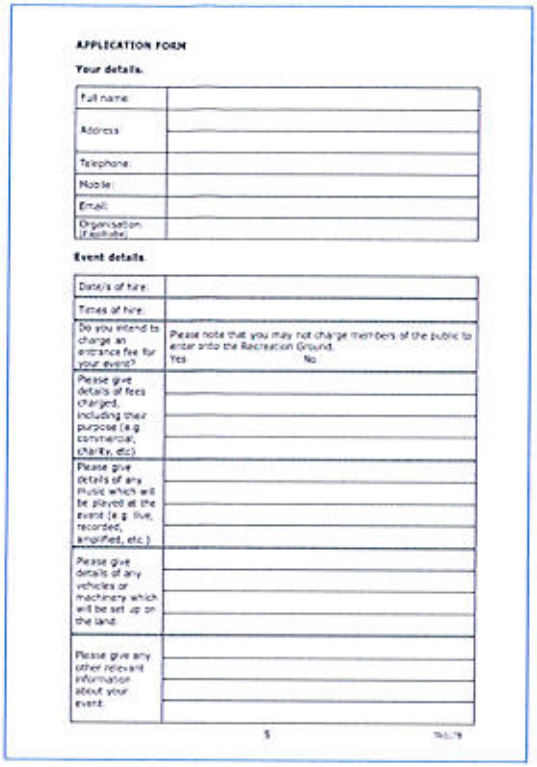
Post Code

Home Telephone Mobile Telephone

Email Address

Which country issued / would issue your passport

	Person 1	Person 2
Primary contact		
Preferred method of contact	Email	Post
Will you be supplying an interpreter for the ceremony?	Yes	No



APPLICATION FORM

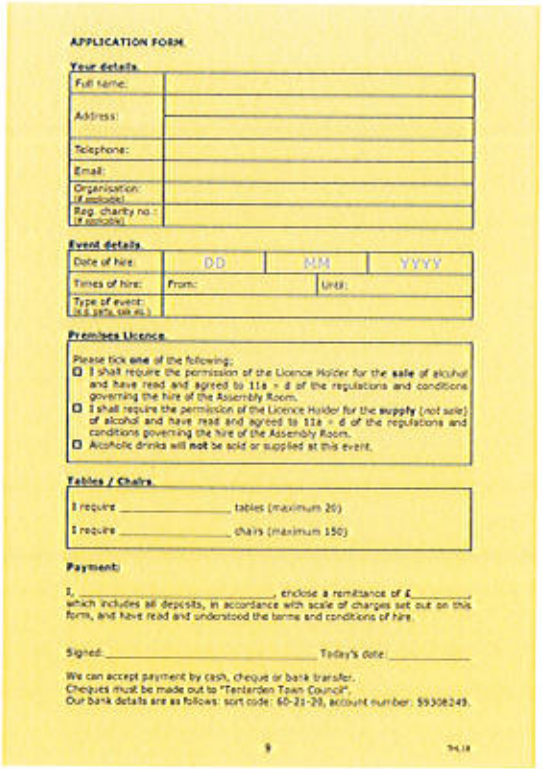
Your details

Full name:	
Address:	
Telephone:	
Mobile:	
Email:	
Organisation: (if applicable)	

Event details

Date/s of hire:	
Times of hire:	
Do you intend to charge an entrance fee for your event?	Please note that you may not charge members of the public to enter onto the Recreation Ground. Yes No
Please give details of fees charged, including their purpose (e.g. commercial, charity, etc)	
Please give details of any music which will be played at the event (e.g. live, recorded, amplified, etc.)	
Please give details of any vehicles or machinery which will be set up on the land	
Please give any other relevant information about your event	

5



APPLICATION FORM

Your details

Full name:	
Address:	
Telephone:	
Email:	
Organisation: (if applicable)	
Reg. charity no.: (if applicable)	

Event details

Date of hire:	DD	MM	YYYY
Times of hire:	From:	Until:	
Type of event: (e.g. party, talk etc.)			

Premises Licence

Please tick **one** of the following:

- ☐ I shall require the permission of the Licence Holder for the **sale** of alcohol and have read and agreed to 11a – d of the regulations and conditions governing the hire of the Assembly Room.
- ☐ I shall require the permission of the Licence Holder for the **supply** (*not sale*) of alcohol and have read and agreed to 11a – d of the regulations and conditions governing the hire of the Assembly Room.
- ☐ Alcoholic drinks will **not** be sold or supplied at this event.

Tables / Chairs

I require _____ tables (maximum 20)

I require _____ chairs (maximum 150)

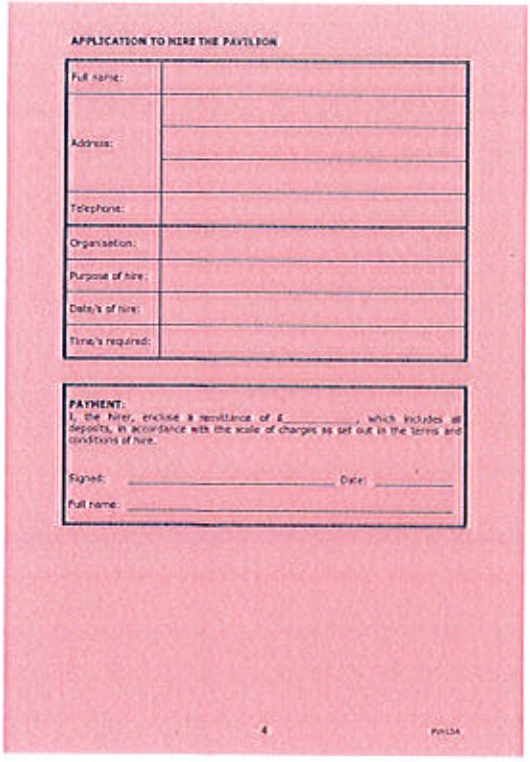
Payment

I, _____, enclose a remittance of £_____ which includes all deposits, in accordance with scale of charges set out on this form, and have read and understood the terms and conditions of hire.

Signed: _____ Today's date: _____

We can accept payment by cash, cheque or bank transfer.
Cheques must be made out to "Tenterden Town Council".
Our bank details are as follows: sort code: 60-21-20, account number: 59308249.

3



APPLICATION TO HIRE THE PAVILION

Full name:	
Address:	
Telephone:	
Organisation:	
Purpose of hire:	
Date/s of hire:	
Time/s required:	

PAYMENT:
I, the hirer, enclose a remittance of £_____, which includes all deposits, in accordance with the scale of charges as set out in the terms and conditions of hire.

Signed: _____ Date: _____

Full name: _____

4

TENTERDEN TOWN COUNCIL

Town Hall, 24 High Street, Tenterden, Kent. TN30 6AN

Website: www.tenterdentowncouncil.gov.uk
Telephone: 01580 762271

Email: townhall@tenterdentowncouncil.gov.uk

PERSONAL DATA BREACH NOTIFICATION POLICY

1. SCOPE

1.1 This procedure applies in the event of a personal data breach under Article 33 Notification of a personal data breach to the supervisory authority, and Article 34 Communication of a personal data breach to the data subject of the GDPR.

1.2 The GDPR draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Therefore, each organisation, should establish whether it is data controller, or a data processor for the same data processing activity; it must be one or the other.

2. RESPONSIBILITY

2.1 All users (whether Employees/Staff, contractors or temporary Employees/Staff and third-party users) and Councillors of Tenterden Town Council are required to be aware of, and to follow this procedure in the event of a personal data breach.

3. PROCEDURE – BREACH NOTIFICATION DATA PROCESSOR TO DATA CONTROLLER

3.1 Tenterden Town Council shall report any personal data breach to the data controller (Clerk) without undue delay who will pass details to the Data Protection Officer. (GDPR-Info Ltd).

3.2 GDPR-*info* Ltd notifies their contact within the data controller, which is recorded in the Internal Breach Register.

3.3 Notification is made by [email, phone call, etc.].

3.4 Confirmation of receipt of this information is made by email.

4. PROCEDURE – BREACH NOTIFICATION DATA CONTROLLER TO SUPERVISORY AUTHORITY

4.1 GDPR-Info Ltd shall notify the supervisory authority [ICO] without undue delay, of a personal data breach.

4.2 GDPR-Info Ltd assesses whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach.

4.3 If a risk to the aforementioned is likely, GDPR-Info Ltd shall report any personal data breach to the supervisory authority without undue delay, and where feasible not later than 72 hours. Where data breach notification to the supervisory authority is not made within 72 hours, it shall be accompanied by the reasons for the delay.

4.4 The data controller (Clerk) shall provide the following information to the supervisory authority on a Breach Notification Form:

(i) A description of the nature of the breach
(ii) The categories of personal data affected
(iii) Approximate number of data subjects affected
(iv) Approximate number of personal data records affected
(v) Name and contact details of GDPR-*info* Ltd
(vi) Likely consequences of the breach
(vii) Any measures that have been or will be taken to address the breach, including mitigation

4.5 The information relating to the data breach, which may be provided in phases.

4.6 GDPR-*info* Ltd notifies their contact within the supervisory authority, which is recorded in the Internal Breach Register.

4.7 Notification is made by [email, phone call, etc.].

4.8 Confirmation of receipt of this information is made by email.

5. PROCEDURE – BREACH NOTIFICATION DATA CONTROLLER TO DATA SUBJECT

5.1 Where the personal data breach is likely to result in high risk to the rights and freedoms of the data subject Tenterden Town Council shall notify the affected data subjects without undue delay, [using this form/in accordance with GDPR-*info* Ltd.'s recommendations].

5.2 The notification to the data subject shall describe in clear and plain language the nature of the breach including the information specified 4.4 above.

5.3 Appropriate measures have been taken to render the personal data unusable to any person who is not authorised to access it, such as encryption.

5.4 The controller has taken subsequent measure to ensure that the rights and freedoms of the data subjects are no longer likely to materialise.

5.5 It would require a disproportionate amount of effort. In such a scenario, there shall be a public communication or similar measure whereby the data subject is informed in an equally effective manner.

5.6 The supervisory authority may where it considers the likelihood of a personal data breach resulting in high risk require the data controller to communicate the personal data breach to the data subject.

TENTERDEN TOWN COUNCIL

Town Hall, 24 High Street, Tenterden, Kent. TN30 6AN

Website: www.tenterdentowncouncil.gov.uk
Telephone: 01580 762271

Email: townhall@tenterdentowncouncil.gov.uk

CCTV POLICY AND CODE OF PRACTICE

Introduction

Closed circuit television (CCTV) is installed at the Council premises for the purpose of staff and premises security. Cameras are located at various places on the premises, and images from the cameras are recorded.

The use of CCTV falls within the scope of the General Data Protection Regulation and the Data Protection Act 2018. In order to comply with the requirements of the law, data must be:

- Fairly and lawfully processed
- Processed for limited purposes and not in any manner incompatible with those purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept for longer than is necessary
- Processed in accordance with individuals' rights
- Secure

Data Protection Statement

1. Tenterden Town Council are the Data Controllers under the Act.

2. CCTV is installed for the purpose of staff, and premises security.

3. Access to stored images will be controlled on a restricted basis within the Council.

4. Use of images, including the provision of images to a third party, will be in accordance with the Councils Data Protection registration.

5. CCTV may be used to monitor the movements and activities of staff and visitors whilst on the premises.

6. CCTV images may be used where appropriate as part of staff counselling or disciplinary procedures.

7. External and internal signage are displayed *on the premises* stating of the presence of CCTV and indicating the names of the Data Controllers and a contact number during office hours for enquiries.

Retention of Images

Images from cameras are recorded a secure hard drive ("the recordings"). Where recordings are retained for the purposes of security of staff and premises, these will be held in secure storage, and access controlled. Recordings which are not required for the purposes of security of staff, and premises, will not be retained for longer than is necessary **(14 day *retention period*).**

The system **has** an automatic power backup facility which may operate in the event of a main supply power failure.

Access to Images

It is important that access to, and disclosure of, images recorded by CCTV and similar surveillance equipment is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes.

Access to Images by Council Staff

Access to recorded images is restricted to *the Data Controllers*, who will decide whether to allow requests for access by data subjects and/or third parties (see below).

Viewing of images must be documented as follows:

- The name of the person removing from secure storage, or otherwise accessing, the recordings
- The date and time of removal of the recordings
- The name(s) of the person(s) viewing the images (including the names and organisations of any third parties)
- The reason for the viewing
- The outcome, if any, of the viewing
- The date and time of replacement of the recordings

Removal of Images for Use in Legal Proceedings

In cases where recordings are removed from secure storage for use in legal proceedings, the following must be documented:

- The name of the person removing from secure storage, or otherwise accessing, the recordings
- The date and time of removal of the recordings
- The reason for removal
- Specific authorisation of removal and provision to a third party
- Any crime incident number to which the images may be relevant
- The place to which the recordings will be taken
- The signature of the collecting police officer, where appropriate
- The date and time of replacement into secure storage of the recordings

Access to Images by Third Parties

Requests for access to images will be made using the 'Application to access to CCTV images' form (which is at **Appendix 1**).

The data controller will assess applications and decide whether the requested access will be permitted. Release will be specifically authorised. Disclosure of recorded images to third parties will only be made in limited and prescribed circumstances. For example, in cases of the prevention and detection of crime, disclosure to third parties will be limited to the following:

- Law enforcement agencies where the images recorded would assist in a specific criminal enquiry
- Prosecution agencies
- Relevant legal representatives
- The press/media, where it is decided that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that decision, the wishes of the victim of an incident should be taken into account
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)

All requests for access or for disclosure should be recorded. If access or disclosure is denied, the reason should be documented as above.

Disclosure of Images to the Media

If it is decided that images will be disclosed to the media (other than in the circumstances outlined above), the images of other individuals must be disguised or blurred so that they are not readily identifiable.

If the CCTV system does not have the facilities to carry out that type of editing, an editing company may need to be used to carry it out. If an editing company is used, then the data controller must ensure that there is a contractual relationship between them and the editing company, and:

- That the editing company has given appropriate guarantees regarding the security measures they take in relation to the images
- The written contract makes it explicit that the editing company can only use the images in accordance with the instructions of the data controllers
- The written contract makes the security guarantees provided by the editing company explicit.

Access by Data Subjects

This is a right of access under the 1998 Act, the GDPR and the DPA 2018. Requests for access to images will be made using the 'Application to access to CCTV images' form (which is at **Appendix 1**). The requestor needs to provide enough information so that they can be identified in the footage, such as a specific date and time, proof of their identity and a description of themselves. Any footage provided may be edited to protect the identities of any other people.

Procedures for Dealing with an Access Request

All requests for access by Data Subjects will be dealt with by the Clerk/DPO. The data controller will locate the images requested. The data controller will determine whether disclosure to the data subject would entail disclosing images of third parties.

The data controller will need to determine whether the images of third parties are held under a duty of confidence. In all circumstances the Council's indemnity insurers will be asked to advise on the desirability of releasing any information.

If third party images are not to be disclosed, the data controllers will arrange for the third-party images to be disguised or blurred. If the CCTV system does not have the facilities to carry out that type of editing, an editing company may need to be used to carry it out. If an editing company is used, then the data controller must ensure that there is a contractual relationship between them and the editing company, and:

- That the editing company has given appropriate guarantees regarding the security measures they take in relation to the images
- The written contract makes it explicit that the editing company can only use the images in accordance with the instructions of the data controllers
- The written contract makes the security guarantees provided by the editing company explicit

The Data Controller will provide a written response to the data subject within **30** days of receiving the request setting out the data controllers' decision on the request.

A copy of the request and response should be retained.

Complaints

Complaints must be in writing and addressed to the Clerk. Where the complainant is a third party, and the complaint or enquiry relates to someone else, the written consent of the data subject is required. All complaints will be acknowledged within seven days, and a written response issued within 21 days.

Appendix 1
Data Protection Act/General Data Protection Regulation
- Application for CCTV Data Access

ALL Sections must be fully completed. Attach a separate sheet if needed.

Name and address of Applicant	
Name and address of "Data Subject" – i.e. the person whose image is recorded	
If the data subject is not the person making the application, please obtain a signed consent from the data subject opposite	Data Subject signature .....
If it is not possible to obtain the signature of the data subject, please state your reasons	
Please state your reasons for requesting the image	
Date on which the requested image was taken	
Time at which the requested image was taken	
Location of the data subject at time image was taken (i.e. which camera or cameras)	
Full description of the individual, or alternatively, attach to this application a range of photographs to enable the data subject to be identified by the operator	
Please indicate whether you (the applicant) will be satisfied by viewing the image only	

On receipt of a fully completed application, a response will be provided as soon as possible and in any event within **30** days.

COUNCIL USE ONLY	COUNCIL USE ONLY
Access granted (tick)	
Access **not** granted (tick)	Reason for not granting access:
Data Controller's name: Signature: Date:	

TENTERDEN TOWN COUNCIL

Town Hall, 24 High Street, Tenterden, Kent. TN30 6AN

Website: www.tenterdentowncouncil.gov.uk
Telephone: 01580 762271

Email: townhall@tenterdentowncouncil.gov.uk

GENERAL PRIVACY NOTICE – INTERNAL POLICY

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 Tenterden Town Council which is the data controller for your data.

Other data controllers the council works with:

- 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 or room, 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 hall rental 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 7 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 visiting this website https://gdpr-info.com/data-protection-contact-form/ or email.

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 site - www.tenterdentowncouncil.gov.uk.This Notice was last updated in June 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 Tenterden Town Council Data Protection Officer: GDPR-Info Ltd

Email: dpo@gdpr-info.com

TENTERDEN TOWN COUNCIL

Town Hall, 24 High Street, Tenterden, Kent. TN30 6AN

Website: www.tenterdentowncouncil.gov.uk
Telephone: 01580 762271

Email: townhall@tenterdentowncouncil.gov.uk

GENERAL PRIVACY NOTICE – WEBSITE POLICY

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 Tenterden Town Council which is the data controller for your data.

Other data controllers the council works with:

- 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 or room, 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 hall rental 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 7 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 visiting this website https://gdpr-info.com/data-protection-contact-form/ or email.

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 site - www.tenterdentowncouncil.gov.uk.This Notice was last updated in June 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 Tenterden Town Council Data Protection Officer: GDPR-Info Ltd

Email: dpo@gdpr-info.com

TENTERDEN TOWN COUNCIL

Town Hall, 24 High Street, Tenterden, Kent. TN30 6AN

Website: www.tenterdentowncouncil.gov.uk
Telephone: 01580 762271

Email: townhall@tenterdentowncouncil.gov.uk

DATA RETENTION AND DISPOSAL POLICY

Date: 1st August 2018

1 Introduction

1.1 The guidelines set out in this document supports the Council's Data Protection Policy and assists us in compliance with the Freedom of Information Act 2000, the General Data Protection Regulation & The Data Protection Act 2018 and other associated legislation.

1.2 It is important that the Council has in place arrangements for the retention and disposal of documents necessary for the adequate management of services in undertaking its responsibilities. This policy sets out the minimum requirements for the retention of documents and sets out the requirements for the disposal of documents. However, it is important to note that this is a live document and will be updated on a regular basis.

1.3 The Council will ensure that information is not kept for longer than is necessary and will retain the minimum amount of information that it requires to carry out its functions and the provision of services, whilst adhering to any legal or statutory requirements.

2 Aims and Objectives

2.1 It is recognised that up to date, reliable and accurate information is a vital to support the work that the Council do and the services that it provides to its residents. This document will help us to:

- Ensure the retention and availability of the minimum amount of relevant information that is necessary for the Council to operate and provide services to the public.
- Comply with legal and regulatory requirements, including the Freedom of Information Act 2000, the Data Protection Act 1998, the General Data Protection Regulation, the Data Protection Act 2018 and the Environmental Information Regulations 2004.
- Save employees' time and effort when retrieving information by reducing the amount of information that may be held unnecessarily. This will assist them as they carry out their daily duties, or if searching for information requested under the Freedom of Information Act.

- Ensure archival records that are of historical value are appropriately retained for the benefit of future generations.

3 Scope

3.1 For the purpose of this Strategy, 'documents' includes electronic, microfilm, microfiche and paper records.

3.2 Where storage is by means of paper records, originals rather than photocopies should be retained where possible.

4 Standards

4.1 The Council will make every effort to ensure that it meets the following standards of good practice:

- Adhere to legal requirements for the retention of information as specified in the Retention Schedule at Annex A. This document provides a framework for good practice requirements for retaining information.
- Personal information will be retained in locked filing cabinets within the Clerk's Office and/or the Senior Assistant's office, access to these documents will only be by authorised personnel.
- Disclosure information will be retained in a locked cabinet in the Clerk's Office.
- Appropriately dispose of information that is no longer required.
- Appropriate measures will be taken to ensure that confidential and sensitive information is securely destroyed.
- Information about unidentifiable individuals is permitted to be held indefinitely for historical, statistical or research purposes e.g. Equalities data.
- Wherever possible only one copy of any personal information will be retained and that will be held within the Clerk's Office or the Senior Assistant's Office.

5 Breach of Policy and Standards

5.1 Any employee who knowingly or recklessly contravenes any instruction contained in, or following from, this Policy and Standards may, depending on the circumstances of the case, have disciplinary action, which could include dismissal, taken against them.

6 Roles and Responsibilities

6.1 The Clerk has overall responsibility for the policy.

6.2 The Clerk is responsible for the maintenance and operation of this policy including ad-hoc checks to ensure compliance.

6.2 Other delegated staff are responsible for ensuring their records are kept and destroyed in line with this policy.

6.3 The Clerk responsible for ensuring that the guidelines set out in this policy are adhered to and to ensure that any documents disposed of are done so in

accordance with their 'sensitivity' (i.e. whether they are normal waste or 'Confidential Waste'

7 Confidential Waste

7.1 Fundamentally any information that is required to be produced under the Freedom of Information Act or Environmental Information Regulations, is available on the website or is open to public inspection should NOT be treated as confidential waste.

7.2 However, any information that is protected by the Data Protection Act or as Confidential under the Councils Constitution should be treated as confidential waste for disposal purposes.

7.3 Examples of what constitutes confidential waste:

- Exempt information contained within committee reports.
- Files containing the personal details of an individual and files that predominantly relate to a particular individual or their circumstances. For example completed application forms and letters.
- Materials given to us on a 'confidential' or on a limited use basis e.g. material provided by contractors or the police.

7.4 Examples of what does not constitute confidential waste:

- Documents that are available to the public via our web site or by submitting an appropriate search request to ourselves for general information.
- All reports and background papers of matters taken to Committee in public session unless specifically exempt

8 Disposal of Documentation

8.1 Confidential waste which clearly shows any personal information or information which can be identified using the parameters set out in 7.3 will be shredded within the council buildings.

9 Retention

9.1 Timeframes for retention of documents have been set using legislative requirements and the Chartered Institute of Personnel and Professional Development (CIPD) guidelines.

9.2 Throughout retention the conditions regarding safe storage and controlled access will remain in place.

9.3 Disclosure information appertaining to Disclosure and Barring Checks must be kept securely in a locked cabinet. Only those entitled to see it in the course of their duties should have access. The security and confidentiality of all Disclosure information is closely registered under the Police Act 1997.

9.4 Disclosure information must not be retained for a period of more than six months and must be destroyed in a secure manner using the shredder in the Reception office.

9.5 Any unauthorised employee accessing or attempting to access Disclosures or Disclosure information or personnel records will be dealt with under the Council's disciplinary procedures.

9.6 The attached 'Appendix' shows the minimum requirements for the retention of documents as determined by those officers responsible for the management of these particular documentation types. Officers holding documents should exercise judgement as to whether they can be disposed of at the end of those periods detailed in the attached 'Appendix'

10 Storage and Access

10.1 Disclosure information is kept separately from personnel files and in securely lockable, non-portable cabinet with access strictly controlled and limited to the Clerk, and/or the Senior Assistant.

11 Handling

11.1 The Council complies with s124 of the Police Act 1997, so that Disclosure Information is only passed to those who are authorised to receive it in the course of their duties. The Council maintains a record of all those to who Disclosures or Disclosure Information has been revealed and recognises that it is a criminal offence to pass this information to anyone who is not entitled to receive it.

11.2 Personal information will only be available to those who are authorised officers.

11.3 Customers' details and information will be kept up to date and reviewed annually by an authorised officer.

12 Usage

12.1 Disclosure information is only used for the specific purpose for which it was requested and for which the applicant's/employee's consent has been given. Disclosure Information will be shared between different areas of the Council, if necessary.

12.2 Where Disclosure information is shared with anyone other than the Clerk, the Senior Assistant and the direct Manager the employee must be given a reason why this information is being shared.

APPENDIX A

Recommended Document Retention Timescales

The retention period should be the number of years specified plus the current financial period (i.e. three years plus the current period, therefore at least three years documentation will always be retained at any given point in time).

This list is not exhaustive; if you are unsure about any document contact the Town Clerk or the Deputy Town Clerk for clarification.

Document Retention Period

Finance

Document	Retention Period
Financial Published Final Accounts	Indefinitely
Signed Audited Accounts	Indefinitely
Final Account working papers	5 years
Records of all accounting transactions held by the Financial Management System	At least 5 years
Cash Books (records of monies paid out and received)	6 years
Purchase Orders	6 years
Cheque Payment Listings (Invoices received)	6 years
Payment Vouchers Capital and Revenue (copy invoices)	6 years
BACS listings	6 years
Goods received notes, advice notes and delivery notes	3 years
Copy receipts	6 years
Petty cash vouchers and reimbursement claims	6 years
Debtors and rechargeable works records	6 years
Expenses and travel allowance claims	6 years
Asset Register for statutory accounting purposes	10 years
Journal Sheets	5 years
Ledger / Trial Balance	10 years
Year end ledger tabulations – ledger details and cost updates	5 years
Published Budget Books	Indefinitely Medium Term
Financial Plan	Indefinitely
Budget Estimates – Detailed Working Papers and summaries	3 years
Bank Statement (Disk Space) and Instructions to banks	6 years
Bank Statements (Hardcopy)	6 years
Banking Records including Giro cheques, bills of exchange and other negotiable instruments	6 years
Prime evidence that money has been banked	6 years
Refer to Drawer (RD) cheques	2 years

Cancelled Expenditure cheques	2 years
Bank Reconciliation	3 years
Cheques presented / drawn on the Council bank accounts	3 years
Prime records that money has been correctly recorded in the Councils financial systems	3 years
Grant/Funding Applications & Claims	5 years
Precept Forms	Indefinitely
Internal Audit Plans/ Reports	3 years
Fees and Charges Schedules	5 years
Time sheets and overtime claims	6 years
Payroll and tax information relating to employees	6 years
Payroll costing analysis	2 years
Records of payment made to employees for salaries / wages (including intermediate payslips)	6 years
Statutory end of year returns to Inland Revenue and Pensions Section	Indefinitely
Loans and Investment Records; temporary loan receipts and loan tabulations	6 years (after redemption of loan)
VAT, Income Tax and National Insurance Records	6 years
Current and expired insurance contracts and policies indefinitely Insurance records and claims	6 years
Capital and contracts register	Indefinitely
Final accounts of contracts executed under hand	6 years from completion of contract
Final accounts of contracts executed under seal	12 years from completion of contract
All Other reconciliations	3 years

Personnel

Unsuccessful application forms	6 months
Unsuccessful reference requests	1 year
Successful application forms and CVs	For duration of employment + 5 years
References received	For duration of employment + 5 years
Statutory sick records, pay, calculations, certificates etc.	For duration of employment + 5 years
Annual leave records	For duration of employment + 5 years
Unpaid leave/special leave	For duration of employment + 5 years
Annual appraisal/assessment records	Current year and previous 2 years
Time Control Records	2 years
Criminal Records Bureau Checks	6 months
Personnel files and training records	5 years after employment ceases

Disciplinary or grievance investigations - proved -Verbal -Written -Final warning - Anything involving children	6 months 1 year 18 months permanently
Disciplinary or grievance investigations - unproven	Destroy immediately after investigation or appeal
Statutory Maternity/Paternity records, calculations, certificates etc	3 years after the tax year in which the maternity period ended
Wages/salary records, overtime, bonuses, expenses etc	6 years

Corporate

Minutes and reports of Committee meetings	Indefinitely
Minutes and reports for Special Committee meetings	Indefinitely
Minutes and reports of sub-committees	Indefinitely
Notes and reports of working groups	Indefinitely
Policies and procedures	Until updated or reviewed
Asset Management records	Indefinitely
Asset management reports	Indefinitely
Internal audit records	3 years
Internal audit fraud investigation	7 years from date of final outcome of investigation
Risk register	Indefinitely
Risk management reports	Indefinitely
Performance reports	Indefinitely
Equalities data	Indefinitely
Questionnaire data	Indefinitely
Details regarding burials	Indefinitely
Drivers log books and mileage	6 years
Vehicle maintenance and registration records (all necessary certificates, MOT certificates, test records and vehicle registration documents etc)	2 years after vehicle disposed of
Fuel usage records	3 years
Allotment application forms	Length of Tenancy + 2 years
Allotment agreements	Length of Tenancy + 2 years
Show health & safety statements	2 Years
Show application including caterers, displays, competition entrants	1 year
Services and equipment quotations – show	1 year
Contacts for show	1 year
Show stalls database inc handcraft and horticulture entrants' details	1 year
trips tenders for coach hire	1 year
Trip database of applicants Coach Tours	1 year
Paper application	1 year

Pre-tender qualification document Summary list of expression of interest received Company contacts A summary of any financial or technical evaluation supplied with the expressions of interest Initial application	1 year
Successful tender documentation Life of contract	6 years
Unsuccessful tender documentation	Until final payment is made
Deeds of land and property	Indefinitely
Land and property rental agreements	6 years after expiry of the agreement
Property evaluation lists	Indefinitely
Lease agreements, variation and valuation queries	6 years after the expiry of the agreement
Documentation referring to externally funded projects	6 years
Booking diaries	3 years
Electronic booking information Is held in the system indefinitely due to the need to gather statistical information	
Premises License applications	Indefinitely

Health & Safety

Health and Safety Accident books	3 years after the date of the last entry (unless an accident involving chemicals or asbestos is contained within
Medical records containing details of employee exposed to asbestos or as specified by the Control of Substances Hazardous to Health Regulations 1999	40 years from the date of the last entry
Medical examination certificates	4 years from date of issue
Records relating to accidents person over 18 years	3 years from date of accident
Records relating to accidents person under 18 years	Until 21st birthday
Asbestos records for premises/property including survey and removal records	40 years
Parks and play area inspection reports	5 years
All inspection certificates (Gas Safe, FENSA etc)	2 years
Repairs job sheets	2 years
Periodic machinery inspection tests (PAT, equipment calibration etc)	2 years
Warranties	10 years
Documents relating to the process of collecting, transporting and disposal of general waste	3 years

Documents relating to the process of collecting, transporting and disposal of hazardous waste	10 years
Plant and equipment testing	2 years
Risk Assessment Forms	2 years
Unusual Incident Forms	3 years
Manual Handling Assessment Forms	3 years

Additional Items	
Approved Minutes	Indefinite
Draft/Rough notes taken at meeting	Until minutes are approved
CCTV	14 days

TENTERDEN TOWN COUNCIL

Town Hall, 24 High Street, Tenterden, Kent. TN30 6AN

Website: www.tenterdentowncouncil.gov.uk
Telephone: 01580 762271

Email: townhall@tenterdentowncouncil.gov.uk

SUBJECT ACCESS REQUEST POLICY

1. Scope

All personal data processed by Tenterden Town Council is within the scope of this procedure. This procedure excludes personal data that is asked for as a matter of routine by data subjects. Data subjects are entitled to ask:

- Whether Tenterden Town Council is processing any personal data about that individual and, if so, to be given:
  - a description of the personal data;
  - the purposes for which it is being processed; and,
  - details of who will be allowed to see the personal data.
- To be given a copy of the information and to be told about the sources from which Tenterden Town Council derived the information; and
- Where appropriate, logic involved in any automated decisions relating to them.

2. Responsibilities

GDPR-*info* Ltd are responsible for the application and effective working of this procedure, and for reporting to the Clerk on Subject Access Requests (SARs). GDPR-*info* Ltd is responsible for handling all SARs.

3. Procedure

3.1 Subject Access Requests must be made using our web page https://gdpr-info.com/data-protection-contact-form/

3.2 The data subject must provide evidence as to identity.

3.3 The data subject must identify the data that is being requested and where it is being held and this information must be shown on the SAR application form. Note that the data subject is entitled to ask for all data that Tenterden Town Council holds, without specifying that data.

3.4 The date by which the identification checks, and the specification of the data sought must be recorded; Tenterden Town Council has one month from this date to provide the requested information. There are no circumstances in which an

extension to that one month will be provided, and failure to provide the requested information within that one month is a breach of the GDPR.

3.5 The SAR application is immediately forwarded to GDPR-info Ltd, who will ensure that the requested data is collected within the time frame.

Collection will entail either:

(i) Collecting the data specified by the data subject, or

(ii) Searching all databases and all relevant filing systems (manual files) in Tenterden Town Council, including all back up and archived files, whether computerised or manual, and including all e-mail folders and archives. The Clerk maintains a data map that identifies where all data in Tenterden Town Council is stored.

3.6 GDPR-info Ltd maintains a record of requests for data and of its receipt, including dates. Note that data may not be altered or destroyed in order to avoid disclosing it.

3.7 GDPR-info Ltd is responsible for reviewing all provided documents to identify whether any third parties are identified in it and for either excising identifying third party information from the documentation or obtaining written consent from the third party for their identity to be revealed.

3.8 If the requested data falls under one of the following exemptions, it does not have to be provided:

(i) Crime prevention and detection.

(ii) Negotiations with the requester.

(iii) Management forecasts.

(iv) Confidential references given by Tenterden Town Council (not ones given to Tenterden Town Council).

(v) Information used for research, historical or statistical purposes.

(vi) Information covered by legal professional privilege.

3.9 The information is provided to the data subject in electronic format unless otherwise requested and all the items provided are listed on a schedule that shows the data subject's name and the date on which the information is delivered.

3.10 The electronic formats used for responses to SARs are:

(i) .CSV file

TENTERDEN TOWN COUNCIL

Town Hall, 24 High Street, Tenterden, Kent. TN30 6AN

Website: www.tenterdentowncouncil.gov.uk
Telephone: 01580 762271

Email: townhall@tenterdentowncouncil.gov.uk

DATA PROTECTION TRAINING POLICY

1. Tenterden Town Council ensures that those with day-to-day responsibility for enabling the demonstration of compliance with the General Data Protection Regulation (GDPR) and good practice are able to demonstrate competence in their understanding of the GDPR and good practice, and how this should be implemented within Tenterden Town Council.

2. The Department keeps records of the relevant training undertaken by each person who has this level of responsibility.

3. Tenterden Town Council also ensures that these staff members remain informed about issues related to the management of personal information, where appropriate, by contact with external bodies. Tenterden Town Council maintains a list of relevant external bodies, the most important of which is the Information Commissioner's Office (www.ico.gov.uk) .

4. Tenterden Town Council ensures that all staff understand their responsibility to ensure that personal information is protected and processed in accordance with Tenterden Town Council's procedures, taking into account any related security requirements.

5. All employees/staff are given training to enable them to process personal information in accordance with Tenterden Town Council's procedures. This training is relevant to the role that each employee performs within Tenterden Town Council.

6. The Clerk is responsible for organising relevant training for responsible individuals and staff generally, and for maintaining records of the attendance of staff at relevant training at appropriate times across Tenterden Town Council's business cycle.