

BOVEY TRACEY TOWN COUNCIL

TOWN HALL • BOVEY TRACEY • NEWTON ABBOT • DEVON TQ13 9EG
Tel: 01626 834217 • E-mail: info@boveytracey.gov.uk • www.boveytracey.gov.uk
Office hours: 10.30am - 12.30pm Mon, Wed. & Fri.

17th April 2018

To Members of the Finance, Resources & General Purposes Committee

Cllrs Gribble (Chairman), Leigh (Deputy Chairman), Ms Blair (Ex Officio), Allen, Evans, Ms Richardson & Robillard.

Cc All other Members of the Council for information.

Dear Councillor,

You are hereby summoned to attend a meeting of the **Finance, Resources and General Purposes (FR&GP) Committee** which will be held in the Council Chamber, Town Hall Bovey Tracey on **Monday 23rd April 2018 at 7pm** for the purpose of transacting the business as set out below.

AGENDA

Interests to be Declared: In accordance with the Code of Conduct, Members are invited to declare any personal or disclosable pecuniary interests, including the nature and extent of such interests, they may have in items to be considered at this meeting. Members are also reminded that any change to their Declaration of Interests must be notified to the Monitoring Officer at Teignbridge District Council within 28 days of the change.

Prior to the commencement of the meeting, Mr Mike Cooke (Chairman of Newton Abbot to Heathfield Railway Revival Group) will be in attendance to provide an update about this project.

FR&GP.18/32 Apologies for absence:

****Public Participation:**

The Committee, at the Chairman's discretion, sets aside a short period of time at the commencement of the meeting when the public can ask questions or make statements regarding agenda items.

FR&GP.18/33 Minutes:

To agree as a correct record and approve the minutes of the meeting of 5th March 2018 (*copy enclosed).

FR&GP.18/34 Accounts & Financial Statement:

To receive and approve payment and receipt transactions between 24th February 2018 and 29th March 2018 (*copy enclosed) and note the bank balances as below;

General Account:	£ 10,923.35	(Statement dated 29.3.18)
Business Bank Instant A/C:	£191,049.04	(Statement dated 29.3.18)
Business Bank Instant A/C:	£350,291.31	(Statement dated 29.3.18)

FR&GP.18/35 General Data Protection Regulation (GDPR):

i) To consider recommending to Full Council the adoption of the following draft documents aiding the Council's compliance towards the new regulations:

- Data Audit Schedule (Inventory of Data Captured) (*copy enclosed)
- Information Data Protection Policy (*copy enclosed)
- Document Retention & Disposal Policy & list of documents for retention or disposal Appendix A (*copy enclosed)
- The Management of Transferable Data Policy (*copy enclosed)
- Social Media Policy (previously adopted June 2016) (*copy enclosed)
- General Privacy Notice (*copy enclosed)
- Subject Access Request (SAR) Policy & (SAR) Form (*copy enclosed)
- Data Security Breach Reporting Form (*copy enclosed)
- Consent Form (*copy enclosed)

ii) To consider the appointment of a Data Protection Officer. The Town Clerk will provide further information at the meeting.

iii) To delegate authority to the Town Clerk to have the authority, if necessary, to spend up to a set budget to ensure that the Town Council is compliant.

FR&GP.18/36 Honorary Representative of the Lord of the Manor 2018/19:

To consider a nomination received (*copy enclosed) for the role of Honorary Representative of the Lord of the Manor for 2018/19.

FR&GP.18/37 Rural Aid Fund - 2018:

To consider an appropriate scheme relevant for an application for Rural Aid. Applications to be submitted by 4pm on Monday 30th April 2018.

FR&GP.18/38 The Councillor Advocate Scheme (CAS):

Item brought forward for discussion by Cllr Leigh and resolve any actions required.

FR&GP.18/39 Annual Governance and Accountability Return - 2017/18:

To consider the Annual Governance Statement (*copy enclosed) for the year ending 31st March 2018 and to recommend to Full Council responses for each of the nine statements of Corporate Governance.

FR&GP.18/40 Matters brought forward by Councillors: (for information only).

**Copies of correspondence circulated to Councillors with this agenda, which will be considered at the meeting.*

SIGNED
M WELLS
TOWN CLERK

DATE 17/04/18

FINANCE, RESOURCES & GENERAL PURPOSES COMMITTEE MEETING
HELD IN THE COUNCIL CHAMBER ON MONDAY 5TH MARCH 2018 AT 7PM

Present:

The Deputy Town Mayor, Cllr Ms J H Blair

Cllr A Allen

Cllr S P Leigh

Cllr G J Gribble**/*

Cllr Ms C O Richardson

In attendance:

Cllr D K Elphick

Mr M Wells - Town Clerk

Mr M Sugden & Mrs M Johnson - Bovey Tracey Youth Action

**County Cllr

*District Cllr

The meeting was chaired by Cllr Gribble

FR&GP.18/21 Apologies for absence:

Cllr M J Evans - Attending another meeting

Cllr C W Robillard - Unwell

**Public Participation:

Mr Sugden and Mrs Johnson spoke in support of item FR&GP.18/27 - Grant for Bovey Tracey Youth Action. Mr Sugden circulated a brief report summarising the current position and verbally presented key aspects of the report. Mr Sugden and Mrs Johnson then answered questions raised by Councillors.

Mr Sugden and Mrs Johnson then left the meeting at 7.20pm.

FR&GP.18/22 Minutes:

The minutes of the meeting of 8th January 2018 (**copy previously circulated*) were confirmed as a correct record and were approved.

FR&GP.18/23 Accounts & Financial Statement:

Members received and approved payment and receipt transactions between 1st January and 23rd February 2018 (**copy previously circulated*) and noted the bank balances as below:

General Account: £ 19,273.28 (Statement dated 13.2.18)

Business Bank Instant A/C: £202,314.90 (Statement dated 2.2.18)

Business Bank Instant A/C: £350,263.00 (Statement dated 2.2.18)

FR&GP.18/24 Fees & Charges 2018/19:

Consideration was given to a review of the current fees and charges (**copy previously circulated*). The Town Clerk outlined the proposed charges.

Resolved:

- i) To delete non-parishioner search fee (part 5 of cemetery fees).
- ii) To approve the proposed fees and charges (**copy attached*) including an amendment from Cllr Leigh to increase the allotment fees (section 2) by 2.5%.

FR&GP.18/25 Newton Abbot to Heathfield Railway Revival Project:

Item brought forward by Cllr Allen (**copy previously circulated*). Cllr Allen referred to his briefing note. Following discussion it was

Resolved:

To invite Mr M Cooke, Chairman of the Newton Abbot to Heathfield Railway Revival Group, to a future FR&GP meeting to present his ideas further. All Councillors will be invited to attend.

FR&GP.18/26 Dartmoor Demon:

Members noted that the Dartmoor Demon cycle ride will take place on Saturday 5th May, passing through Bovey Tracey.

FR&GP.18/27 Grant - Bovey Youth Action:

Consideration was given to a review of the current grant (£7500.00 p.a). The current grant agreement expires on 31st March 2018. Following discussion around the possibility of increasing the current level of grant it was

Resolved:

To recommend to Full Council that the grant remains at £7,500.00 for 2018/19. The Town Clerk will invite the Youth Café to apply to Councillors' Community Fund if additional grant support is required.

FR&GP.18/28 Fly a Flag for the Commonwealth - 12th March 2018:

Consideration was given to an invitation from Bruno Peek (Commonwealth Pageantmaster) to take part in the "Fly a Flag for the Commonwealth" celebrations, by flying the Commonwealth Flag from the Town Hall on Monday 12th March 2018.

Resolved:

To take part, as set out above.

FR&GP.18/29 Elector Fund 2017/18:

Members noted that application for the following Elector Fund grants were successful:

£ 870.00 - CCTV upgrade
£ 870.00 - Purchase of park litter bins
£2000.00 - Bovey Community Care Project
£1000.00 - Neighbourhood Development Plan activities
£2000.00 - Contribution towards the Information Centre temporary relocation costs

FR&GP.18/30 Financial Regulations:

The Town Clerk updated Members on the requirements to review current Financial Regulations (**copy previously circulated*) annually. Members noted that there had been no updates from NALC.

Resolved:

To confirm that the current Financial Regulations remain appropriate.

FR&GP.18/31 Matters brought forward by Councillors: (*for information only*).

Cllr Elphick:

i) Noted his interest in the possible re-opening of the Newton Abbot to Heathfield railway line and looks forward to the forthcoming presentation.

ii) Reported the Heathfield Community Centre Committee wish to reinstate the lift to ensure that people with mobility issues will be able to leave the 1st floor in the event of a fire. He noted that the cost will be £2,000.00. Cllr Gribble offered to attend the next Heathfield Community Centre Committee meeting to discuss possible funding.

Cllr Allen enquired when the Quality Update and Neighbourhood Development Plan questionnaire will be circulated. The Town Clerk confirmed that circulation will take place this week.

The meeting closed at 7.45pm.

List of Payments made between 24/02/2018 and 31/03/2018

<u>Date Paid</u>	<u>Payee Name</u>	<u>Reference</u>	<u>Amount Paid</u>	<u>Authorized Ref</u>	<u>Transaction Detail</u>
01/03/2018	C Beresford	329	40.00		Cleaning
01/03/2018	Devon Contract Waste	330	15.60		Service
01/03/2018	Mole Valley Farmers	331	152.92		Goods
01/03/2018	S W Water Ltd	332	14.05		Supply- Heathfield Youth
01/03/2018	EMS Waste Services Ltd	333	600.00		Skips x 2
01/03/2018	Teignbridge District Council	334	4,252.06		Payroll
01/03/2018	BHGS Hayle	335	468.48		Compost etc
01/03/2018	Newton Abbot Security Trust	336	500.00		CCTV monitoring
01/03/2018	Aviva	D/D	608.18		Insurance
01/03/2018	Pulse8Communications	D/D	22.00		Broadband
07/03/2018	UK Fuels Ltd	D/D	117.69		Fuel
13/03/2018	N Brock	337	374.00		Gravedigging R Harrison
13/03/2018	K & H Harvey	338	819.00		Hedgetrimming
13/03/2018	Teignbridge District Council	339	5,300.00		Payroll
13/03/2018	Specialist Hygiene Services Lt	340	283.64		Cleaning Rec. Grd . toilets
13/03/2018	S West Grounds Maintenance	341	1,800.00		Hedgecutting
13/03/2018	Lee Merry	342	94.34		Reimbursement Banner
13/03/2018	Mrs M Edwards	343	29.99		Reimbursement printing
13/03/2018	Civil Solutions Ltd	344	21.60		Goods
13/03/2018	Royal Mail Group Ltd	345	116.40		Response licence service
13/03/2018	Devon Contract Waste	346	17.28		Collection
13/03/2018	Marketing Solutions	347	947.00		QU & questionnaire delivery
13/03/2018	Mole Valley Farmers	13.3.18	42.13		Goods
13/03/2018	PHS Group	349	246.48		Collection
13/03/2018	Smith Consult Ltd	350	1,303.80		Prep & brief
13/03/2018	Glason UK Ltd	351	941.46		Bins
13/03/2018	Randall Simmonds LLP	352	1,200.00		QS consultancy
19/03/2018	British Gas	D/D	24.17		Electricity supply - cemetery
21/03/2018	EE Phone	D/D	33.44		Plan charge
23/03/2018	Mole Valley Farmers	353	110.44		Goods
23/03/2018	Devon Contract Waste Ltd	354	15.60		Service
23/03/2018	Terence Morgan	355	100.00		Deposit stage G M Festival
23/03/2018	Bovey Court Garage	356	198.22		Repairs
23/03/2018	WPS Ltd	557	467.40		Vehicle insurance
23/03/2018	PVM Supplies Ltd	358	133.49		Goods
23/03/2018	BT Youth Action	359	1,250.00		Grant
23/03/2018	Devon Assoc. of Local Councils	360	48.00		Course attendance
27/03/2018	C Beresford	361	40.00		Cleaning
27/03/2018	P J Bevans	362	292.98		Repairs Heathfield Youth Cabin
27/03/2018	Firewatch SW Ltd	363	192.78		Signs - NDP
27/03/2018	Teignbridge District Council	364	1,721.89		Teignbridge District Council
27/03/2018	PHS Group	365	72.00		Service
28/03/2018	Elitegroup	D/D	58.08		Telecom

Date: 13/04/2018

Bovey Tracey Town Council

Page 2

Time: 10:57

Current Account

List of Payments made between 24/02/2018 and 31/03/2018

<u>Date Paid</u>	<u>Payee Name</u>	<u>Reference</u>	<u>Amount Paid</u>	<u>Authorized Ref</u>	<u>Transaction Detail</u>
------------------	-------------------	------------------	--------------------	-----------------------	---------------------------

		Total Payments	<u>25,086.59</u>		
--	--	-----------------------	------------------	--	--

Current Account

Receipts received between 24/02/2018 and 31/03/2018

Nominal Ledger Analysis

<u>Receipt Ref</u>	<u>Name of Payer</u>	<u>£ Amnt Received</u>	<u>£ Debtors</u>	<u>£ VAT</u>	<u>A/c</u>	<u>Centre</u>	<u>£ Amount</u>	<u>Transaction Detail</u>
358	Banked: 05/03/2018	247.50						
89	Mr P Kennedy-Bruyneels	50.00			1200	100	50.00	Allot 38 - rent 2018
90	Mrs R E Darnell	70.00			1200	100	70.00	Allot 14A Deposit & rent
91	Angel Home Care	120.00			1900	710	120.00	P A testing
92	Western Power Distribution	7.50			1900	100	7.50	Substation lease
359	Banked: 22/03/2018	384.00						
93	BT Cricket Club	137.50			1900	100	137.50	Contribution skip hire
94	Samuel Croker Almshouses	112.50			1900	100	112.50	Contribution skip hire
95	BT Bowling Club	10.00			1900	100	10.00	Annual rent
0510	Mrs K Lewis	124.00			1400	400	124.00	Additional inscription B
360	Banked: 29/03/2018	588.00						
96	Angel Care Ltd	210.00			1900	100	210.00	Hire Council Chamber
0511	Parkers Funeral Directors	378.00			1400	400	378.00	Headstone - B Wombwell
Total Receipts:		1,219.50	0.00	0.00			1,219.50	

1. What Personal Data Do We Hold?													2. Lawful basis for holding personal data			3. Consent		4. Sharing Personal Data		5. Our Internal processes				6. Action Needed
To whom does it relate?	What Data is it?	Including Sensitive Data?	What is it for?	Why do we have it?	Are we legally obliged to hold this data? NOTE: If we are legally obliged to hold it, no consent is needed.	Have we got a contract or privacy notice relating to the data subject?	If we have a contract with the data subject, does it demonstrate all necessary consents?	With whom do we share this data? LIST THEM ALL	Who is responsible for keeping it?	How often is it checked?	How long do we keep it?	Where is it held?	Protection?	Action needed										
Staff	Employment contracts	Yes	HR	It is a contract	No	Contract	Yes	N/A	Clerk	On appointment	Duration of Employment plus 6 years	Filing cabinet	lock and key											
	Leave/sickness record	No	HR	Employment Purposes	No	Yes	Yes	HMRC; payroll provider (eg Teignbridge DC)	Clerk	Monthly	last financial year	Filing cabinet	lock and key											
	Discipline/Grievance record	Yes	HR	Employment	No	Yes	Yes	N/A	Clerk	As required	duration of employment	Filing cabinet	lock and key											
	Next of kin details	Yes	HR	Employment	No	Yes	Yes	N/A	Clerk	As required	duration of employment	Filing cabinet	lock and key											
	Accident/Injury record	No	HR	H&S	Yes	Contract	Yes	N/A	Clerk	As required	doc retention policy	Open shelf	no											
	Pension details	Yes	HR	Legislative requirement	Yes	Contract	Yes	HMRC; payroll provider (eg Teignbridge DC)	Clerk	As required	duration of employment	Filing cabinet	lock and key											
	PAYE	No	HR	Legislative requirement	Yes	Not required	?	HMRC; payroll provider (eg Teignbridge DC)	Clerk	As required	duration of employment	Filing cabinet	lock and key											
	Contact details	Yes	HR	Employment	No	Privacy Notice	Yes	HMRC; payroll provider (eg Teignbridge DC)	Clerk	As required	duration of employment	Filing cabinet and Server	lock and key and password	Privacy Notice to be prepared										
	Bank details	No	HR	To pay staff salaries	No	Contract	Yes	Payroll provider (eg Teignbridge DC)	Clerk	As required	duration of employment	Filing cabinet and Server	lock and key and password											
	Job applications (unsuccessful applicants)	Yes	HR	Employment	No	Yes	Yes	N/A	Clerk	On application	until appointment made	Filing cabinet	lock and key											
Councillors	Job applications/references (successful applicants)	Yes	HR	Employment	No	Yes	Yes	N/A	Clerk	On appointment	duration of employment	Filing cabinet	lock and key											
	Staff Appraisals	Yes	HR	Employment	No	Yes	Yes	N/A	Clerk	As required	duration of employment	Filing cabinet	lock and key											
Contractors/Suppliers	Declarations of Interest	Yes	Democracy	legislative requirement	Yes	Not required	Yes	This is Public Knowledge	All Staff	At election	term of office	Open shelf and website	no											
	Personal contact details	No	Democracy	legislative requirement	Yes	Not required	Yes	This is Public Knowledge	All staff	At election	term of office	Filing cabinet and Server	lock and key and password											
	Email Addresses	No	Democracy	legislative requirement	Yes	Not required	Yes	Internal or external with permissions	All staff	At election	term of office	Server	password											
Residents	Contact details	No	Business	Contact	No	Contract	Yes	External Professional Advisers	Clerk	When appointed	2 years from last contract	Accounts software	password											
	Invoices	No	Business	Payment	No	Contract	Yes	Public inspection on audit	Clerk	On payment	doc retention policy	Accounts software	password											
	Quotations	No	Business	Purchasing	No	Contract	Yes	Public inspection on audit	All staff	On raising	doc retention policy	Files	no											
	Bank Account details	No	Business	Payment	No	Contract	Yes	Our Bank	Clerk	On payment	doc retention policy	Filing cabinet	lock and key											
	Insurance	No	Business	Contact	No	Contract	Yes	External professional advisers	Clerk	On appointment	doc retention policy	Filing cabinet	lock and key											
	References	No	Business	Contact	No	Contract	Yes	External professional advisers	Clerk	On appointment	doc retention policy	Filing cabinet	lock and key											
	Complaints/Compliments	Sometimes	Democracy	Democracy	Democracy	No	Privacy Notice	No contract	External professional advisers	All staff	On receipt	1 year	Filing cabinet	lock and key	Privacy Notice to be prepared									
Community Organisations	Freedom of Information requests	No	Democracy	Democracy	Yes	Privacy Notice	No contract	External Professional Advisers	Clerk	On receipt	doc retention policy	Filing cabinet	lock and key	Privacy Notice to be prepared										
	Electoral Register	No	Democracy	Democracy	No	Not applicable	No contract	Public Document required by law, which we choose to hold.	All staff	On receipt	1 year	Filing cabinet	lock and key											
Allotments	Email Addresses	No	Democracy	Contact	No	Privacy Notice	No Contract	Nobody without consent	All staff	Annually	2 years	Server	password	Privacy Notice to be prepared										
	Grant Application Forms	Perhaps	Democracy	Service to Community	No	Privacy Notice	No Contract	External Professional Advisers	All staff	Annually	2 years	Server	password	Privacy Notice to be prepared										
	Nominations of external committee members	No	Democracy	Contact	No	Privacy Notice	No Contract	Names become Public Knowledge, other data is confidential	All Staff	On appointment	See document Retention Policy	Server	password	Privacy Notice to be prepared										
Cemetery	Waiting list	No	Business	Allocation	No	Privacy Notice	No Contract	Nobody without consent	Clerk	Annually	Until plot available	Filing cabinet	lock and key	Privacy Notice to be prepared										
	Tenant Contact Details	No	Property records	Contact	No	Tenancy Agreement	Yes	Nobody without consent	Clerk	Annually	Indefinite	Filing cabinet	lock and key											
	Tenancy Agreements	No	Property records	Service to Community	No	Tenancy Agreement	Yes	Nobody without consent	Clerk	Annually	until plot relinquished	Filing cabinet	lock and key											
Civic Lists	Record of Burials	No	legal	Legislative requirement	Yes	Not applicable	Not applicable	Public document required by law	Clerk	On purchase	Indefinite	Filing cabinet	lock and key											
	Purchased Graves	Sometimes	legal	Contract	No	Contract	Yes	Any reasonable request	Clerk	On purchase	Indefinite	Filing cabinet	lock and key											
Events	Contact details of Known Undertakers	No	Cemetery Functions	Contact	No	We need a privacy notice	Not applicable	Bereaved families	Clerk	On purchase	Indefinite	Filing cabinet	lock and key											
	Contact details	No	Mayoral functions	Invitations	No	Privacy Notice	No Contract	Nobody without consent	Clerk	Annually	1 year	Filing cabinet	lock and key	Privacy Notice to be prepared										
Planning	Trader Contact Details	No	Business	Contact	No	Privacy Notice	Not applicable	Nobody without consent	Clerk	Each event	1 year	Filing cabinet	lock and key	Privacy Notice to be prepared										
	Objections	No	Democracy	We are consulted on applications	Yes	Public Document	No contract	Our objection /observations is a public document	Clerk	On receipt	1 year	Filing cabinet	lock and key											
Property	Leases/licenses	No	Property	Council function	No	Public Document	Yes	Public Document registered at Land Registry	Clerk	Annually	Indefinitely	Safe	lock and key											
	Tenant Contact Details	No	Democracy	Contact	No	Contract	Yes	External Professional Advisers	Clerk	Annually	See document Retention Policy	Filing cabinet	lock and key											
	Covenants	No	Property	Council function	No	Public Document	Yes	Public Document registered at Land Registry	Clerk	Annually	See document Retention Policy	Filing cabinet	lock and key											
	Public rights of way	No	Property	Council function	No	Public Document	Yes	Public Document registered at Land Registry	Clerk	Annually	See document Retention Policy	Filing cabinet	lock and key											
General Contacts	Service level agreements	No	Property records	Service to Community	No	Tenancy Agreement	Yes	External Professional Advisers	Clerk	Annually	See document Retention Policy	Filing cabinet	lock and key											
	Contact details	No	Democracy	Contact	No	Privacy Notice	Not applicable	Nobody without consent	All staff	On appointment	Duration of plan making	Filing cabinet	lock and key	Privacy Notice to be prepared										
Neighbourhood Development Plan	Email Addresses	Yes	Democracy	Contact	Yes	Privacy Notice	Not applicable	Any reasonable request	All staff	Annually	1 year	Server	password	Privacy Notice to be prepared										
	Contact details	No	Democracy	Contact	No	Privacy Notice	Not applicable	Nobody without consent	All staff	On appointment	Duration of plan making	Filing cabinet	lock and key	Privacy Notice to be prepared										

Bovey Tracey Town Council

Information & Data Protection Policy



Introduction

In order to conduct its business, services and duties, Bovey Tracey Town Council processes a wide range of data, relating to its own operations and some which it handles on behalf of partners. In broad terms, this data can be classified as:

- Data shared in the public arena about the services it offers, its mode of operations and other information it is required to make available to the public.
- Confidential information and data not yet in the public arena such as ideas or policies that are being worked up.
- Confidential information about other organisations because of commercial sensitivity.
- Personal data concerning its current, past and potential employees, Councillors, and volunteers.
- Personal data concerning individuals who contact it for information, to access its services or facilities or to make a complaint.

Bovey Tracey Town Council will adopt procedures and manage responsibly, all data which it handles and will respect the confidentiality of both its own data and that belonging to partner organisations it works with and members of the public. In some cases, it will have contractual obligations towards confidential data, but in addition will have specific legal responsibilities for personal and sensitive information under data protection legislation.

This Policy is linked to our Quality Policy and ICT Policy which will ensure information considerations are central to the ethos of the organisation.

The Town Council will periodically review and revise this policy in the light of experience, comments from data subjects and guidance from the Information Commissioners Office.

The Council will be as transparent as possible about its operations and will work closely with public, community and voluntary organisations. Therefore, in the case of all information which is not personal or confidential, it will be prepared to make it available to partners and members of the Town's communities. Details of information which is routinely available is contained in the Council's Publication Scheme which is based on the statutory model publication scheme for local councils.

Protecting Confidential or Sensitive Information

Bovey Tracey Town Council recognises it must at times, keep and process sensitive and personal information about both employees and the public, it has therefore adopted this policy not only to meet its legal obligations but to ensure high standards.

The General Data Protection Regulation (GDPR) which became law on 25th May 2018 and will like the Data Protection Act 1998 before them, seek to strike a balance between the rights of individuals and the

sometimes, competing interests of those such as the Town Council with legitimate reasons for using personal information.

The policy is based on the premise that Personal Data must be:

- Processed fairly, lawfully and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Data Protection Terminology

Data subject - means the person whose personal data is being processed.

That may be an employee, prospective employee, associate or prospective associate of BTC or someone transacting with it in some way, or an employee, Member or volunteer with one of our clients, or persons transacting or contracting with one of our clients when we process data for them.

Personal data - means any information relating to a natural person or data subject that can be used directly or indirectly to identify the person.

It can be anything from a name, a photo, and an address, date of birth, an email address, bank details, and posts on social networking sites or a computer IP address.

Sensitive personal data - includes information about racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, medical information, sexual orientation, genetic and biometric data or information related to offences or alleged offences where it is used to uniquely identify an individual.

Data controller - means a person who (either alone or jointly or in common with other persons) (e.g. Town Council, employer, council) determines the purposes for which and the manner in which any personal data is to be processed.

Data processor - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Processing information or data - means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organising, adapting or altering it
- retrieving, consulting or using the information or data
- disclosing the information or data by transmission, dissemination or otherwise making it available
- aligning, combining, blocking, erasing or destroying the information or data. regardless of the Technology used.

Bovey Tracey Town Council processes **personal data** in order to:

- fulfil its duties as an employer by complying with the terms of contracts of employment, safeguarding the employee and maintaining information required by law.
- pursue the legitimate interests of its business and its duties as a public body, by fulfilling contractual terms with other organisations, and maintaining information required by law.
- monitor its activities including the equality and diversity of its activities
- fulfil its duties in operating the business premises including security
- assist regulatory and law enforcement agencies
- process information including the recording and updating details about its Councillors, employees, partners and volunteers.
- process information including the recording and updating details about individuals who contact it for information, or to access a service, or make a complaint.
- undertake surveys, censuses and questionnaires to fulfil the objectives and purposes of the Council.
- undertake research, audit and quality improvement work to fulfil its objects and purposes.
- carry out Council administration.

Where appropriate and governed by necessary safeguards we will carry out the above processing jointly with other appropriate bodies from time to time.

The Council will ensure that at least one of the following conditions is met for personal information to be considered fairly processed:

- The individual has consented to the processing
- Processing is necessary for the performance of a contract or agreement with the individual
- Processing is required under a legal obligation
- Processing is necessary to protect the vital interests of the individual
- Processing is necessary to carry out public functions
- Processing is necessary in order to pursue the legitimate interests of the data controller or third parties.

Particular attention is paid to the processing of any **sensitive personal information** and the Town Council will ensure that at least one of the following conditions is met:

- Explicit consent of the individual
- Required by law to process the data for employment purposes
- A requirement in order to protect the vital interests of the individual or another person

Who is responsible for protecting a person's personal data?

The Town Council as a corporate body has ultimate responsibility for ensuring compliance with the Data Protection legislation. The Council has delegated this responsibility day to day to the Town Clerk.

- Email: Info@boveytracey.gov.uk
- Phone: 01626 834217
- Correspondence: The Town Clerk, Town Hall, Town Hall Place, Bovey Tracey, TQ13 9EG

The Town Council has also appointed an external Data Protection Officer to ensure compliance with Data Protection legislation who may be contacted at: IAC Audit & Consultancy Ltd (kevin.rose@audit-iac.com)

Diversity Monitoring

Bovey Tracey Town Council monitors the diversity of its employees, and Councillors, in order to ensure that there is no inappropriate or unlawful discrimination in the way it conducts its activities. It undertakes similar data handling in respect of prospective employees. This data will always be treated as confidential. It will only be accessed by authorised individuals within the Council and will not be disclosed to any other bodies or individuals. Diversity information will never be used as selection criteria and will not be made available to others involved in the recruitment process. Anonymised data derived from diversity monitoring will be used for monitoring purposes and may be published and passed to other bodies.

The Council will always give guidance on personnel data to employees, councillors, partners and volunteers through a Privacy Notice and ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request.

Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Personal data shall not be transferred to a country or territory outside the European Economic Areas unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Information provided to us

The information provided (personal information such as name, address, email address, phone number) will be processed and stored so that it is possible for us to contact, respond to or conduct the transaction requested by the individual. By transacting with Bovey Tracey Town Council, individuals are deemed to be giving consent for their personal data provided to be used and transferred in accordance with this policy, however where ever possible specific written consent will be sought. It is the responsibility of those individuals to ensure that the Town Council is able to keep their personal data accurate and up-to-date. The personal information will be not shared or provided to any other third party or be used for any purpose other than that for which it was provided.

The Councils Right to Process Information

General Data Protection Regulations (and Data Protection Act) Article 6 (1) (a) (b) and (e)

Processing is with consent of the data subject, or

Processing is necessary for compliance with a legal obligation.

Processing is necessary for the legitimate interests of the Council.

Information Security

The 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 appropriate 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.

Children

We will not process any data relating to a child (under 13) without the express parental/ guardian consent of the child concerned.

Rights of a Data Subject

Access to Information: an individual has the right to request access to the information we have on them. They can do this by contacting our Town Clerk or Data Protection Officer:

Information Correction: If they believe that the information we have about them is incorrect, they may contact us so that we can update it and keep their data accurate. Please contact: Town Clerk.

Information Deletion: If the individual wishes the Town Council to delete the information about them, they can do so by contacting the Town Clerk.

Right to Object: If an individual believes their data is not being processed for the purpose it has been collected for, they may object by contacting the Town Clerk or Data Protection Officer.

The Town Council does not use automated decision making or profiling of individual personal data.

Complaints: If an individual has a complaint regarding the way their personal data has been processed, they may make a complaint to the Town Clerk, Data Protection Officer or the Information Commissioners Office casework@ico.org.uk Tel: 0303 123 1113.

The Council will always give guidance on personnel data to employees through the Employee handbook.

The Council will ensure that individuals on whom personal information is kept are aware of their rights and have easy access to that information on request.

Making Information Available

The Publication Scheme is a means by which the Council can make a significant amount of information available routinely, without waiting for someone to specifically request it. The scheme is intended to encourage local people to take an interest in the work of the Council and its role within the community.

In accordance with the provisions of the Freedom of Information Act 2000, this Scheme specifies the classes of information which the Council publishes or intends to publish. It is supplemented with an Information Guide which will give greater detail of what the Council will make available and hopefully make it easier for people to access it.

All formal meetings of Council and its committees are subject to statutory notice being given on notice boards, the Website and sent to the local media. The Council publishes an annual programme in May each year. All formal meetings are open to the public and press and reports to those meetings and relevant background papers are available for the public to see. The Council welcomes public participation and has a public participation session on each Council and committee meeting. Details can be seen in the Council's Standing Orders, which are available on its Website or at its Offices.

Occasionally, Council or committees may need to consider matters in private. Examples of this are matters involving personal details of staff, or a particular member of the public, or where details of commercial/contractual sensitivity are to be discussed. This will only happen after a formal resolution has been passed to exclude the press and public and reasons for the decision are stated. Minutes from all formal meetings, including the confidential parts are public documents.

The Openness of Local Government Bodies Regulations 2014 requires written records to be made of certain decisions taken by officers under delegated powers. These are not routine operational and administrative decisions such as giving instructions to the workforce or paying an invoice approved by Council, but would include urgent action taken after consultation with the Chairman, such as responding to a planning application in advance of Council. In other words, decisions which would have been made by Council or committee had the delegation not been in place.

The 2014 Regulations also amend the Public Bodies (Admission to Meetings) Act 1960 to allow the public or press to film, photograph or make an audio recording of council and committee meetings normally open to the public. The Council will where possible facilitate such recording unless it is being disruptive. It will also take steps to ensure that children, the vulnerable and members of the public who object to being filmed are protected without undermining the broader purpose of the meeting.

The Council will be pleased to make special arrangements on request for persons who do not have English as their first language or those with hearing or sight difficulties.

Disclosure Information

The Council will as necessary undertake checks on both staff and Members with the the Disclosure and Barring Service and will comply with their Code of Conduct relating to the secure storage, handling, use, retention and disposal of Disclosures and Disclosure Information. It will include an appropriate operating procedure in its integrated quality management system.

Data Transparency

The Council has resolved to act in accordance with the Code of Recommended Practice for Local Authorities on Data Transparency (September 2011). This sets out the key principles for local authorities in creating greater transparency through the publication of public data and is intended to help them meet obligations of the legislative framework concerning information.

“Public data” means the objective, factual data on which policy decisions are based and on which public services are assessed, or which is collected or generated in the course of public service delivery.

The Code will therefore underpin the Council’s decisions on the release of public data and ensure it is proactive in pursuing higher standards and responding to best practice as it develops.

The principles of the Code are:

Demand led: new technologies and publication of data should support transparency and accountability

Open: the provision of public data will be integral to the Council’s engagement with residents so that it drives accountability to them.

Timely: data will be published as soon as possible following production.

Government has also issued a further Code of Recommended Practice on Transparency, compliance of which is compulsory for parish councils with turnover (gross income or gross expenditure) not exceeding £25,000 per annum. These councils will be exempt from the requirement to have an external audit from April 2017. Bovey Tracey Town Council exceeds this turnover but will nevertheless ensure the following information is published on its Website for ease of access:

- All transactions above £100.
- End of year accounts
- Annual Governance Statements
- Internal Audit Reports
- List of Councillor or Member responsibilities
- Details of public land and building assets
- Draft minutes of Council and committees within one month
- Agendas and associated papers no later than three clear days before the meeting.

DRAFT

Adopted by Bovey Tracey Town Council:
Review Date:

Bovey Tracey Town Council



Retention and Disposal Policy

1. Introduction

- 1.1 The Council accumulates a vast amount of information and data during the course of its everyday activities. This includes data generated internally in addition to information obtained from individuals and external organisations. This information is recorded in various different types of document.
- 1.2 Records created and maintained by the Council are an important asset and as such measures need to be undertaken to safeguard this information. Properly managed records provide authentic and reliable evidence of the Council's transactions and are necessary to ensure it can demonstrate accountability.
- 1.3 Documents may be retained in either 'hard' paper form or in electronic forms. For the purpose of this policy, 'document' and 'record' refers to both hard copy and electronic records.
- 1.4 It is imperative that documents are retained for an adequate period of time. If documents are destroyed prematurely the Council and individual officers concerned could face prosecution for not complying with legislation and it could cause operational difficulties, reputational damage and difficulty in defending any claim brought against the Council.
- 1.5 In contrast to the above the Council should not retain documents longer than is necessary. Timely disposal should be undertaken to ensure compliance with the General Data Protection Regulations so that personal information is not retained longer than necessary. This will also ensure the most efficient use of limited storage space.

2. Scope and Objectives of the Policy

- 2.1 The aim of this document is to provide a working framework to determine which documents are:
 - Retained – and for how long; or
 - Disposed of – and if so by what method.
- 2.2 There are some records that do not need to be kept at all or that are routinely destroyed in the course of business. This usually applies to information that is duplicated, unimportant or only of a short-term value. Unimportant records of information include:
 - 'With compliments' slips.
 - Catalogues and trade journals.
 - Non-acceptance of invitations.
 - Trivial electronic mail messages that are not related to Council business.
 - Requests for information such as maps, plans or advertising material.
 - Out of date distribution lists.
- 2.3 Duplicated and superseded material such as stationery, manuals, drafts, forms, address books and reference copies of annual reports may be destroyed.
- 2.4 Records should not be destroyed if the information can be used as evidence to prove that something has happened. If destroyed the disposal needs to be disposed of under the General Data Protection Regulations

3. Roles and Responsibilities for Document Retention and Disposal

- 3.1 Councils are responsible for determining whether to retain or dispose of documents and should undertake a review of documentation at least on an annual basis to ensure that any unnecessary documentation being held is disposed of under the General Data Protection Regulations.
- 3.2 Councils should ensure that all employees are aware of the retention/disposal schedule.

4. Document Retention Protocol

- 4.1 Councils should have in place an adequate system for documenting the activities of their service. This system should take into account the legislative and regulatory environments to which they work.
- 4.2 Records of each activity should be complete and accurate enough to allow employees and their successors to undertake appropriate actions in the context of their responsibilities to:
- Facilitate an audit or examination of the business by anyone so authorised.
 - Protect the legal and other rights of the Council, its clients and any other persons affected by its actions.
 - Verify individual consent to record, manage and record disposal of their personal data.
 - Provide authenticity of the records so that the evidence derived from them is shown to be credible and authoritative.
- 4.3 To facilitate this the following principles should be adopted:
- Records created and maintained should be arranged in a record-keeping system that will enable quick and easy retrieval of information under the General Data Protection Regulations
 - Documents that are no longer required for operational purposes but need retaining should be placed at the records office.
- 4.4 The retention schedules in Appendix A: List of Documents for Retention or Disposal provide guidance on the recommended minimum retention periods for specific classes of documents and records. These schedules have been compiled from recommended best practice from the Public Records Office, the Records Management Society of Great Britain and in accordance with relevant legislation.
- 4.5 Whenever there is a possibility of litigation, the records and information that are likely to be affected should not be amended or disposed of until the threat of litigation has been removed.

5. Document Disposal Protocol

- 5.1 Documents should only be disposed of if reviewed in accordance with the following:
- Is retention required to fulfil statutory or other regulatory requirements?
 - Is retention required to meet the operational needs of the service?
 - Is retention required to evidence events in the case of dispute?
 - Is retention required because the document or record is of historic interest or intrinsic value?
- 5.2 When documents are scheduled for disposal the method of disposal should be appropriate to the nature and sensitivity of the documents concerned. A record of the disposal will be kept to comply with the General Data Protection Regulations.
- 5.3 Documents can be disposed of by any of the following methods:
- Non-confidential records: place in waste paper bin for disposal.

- Confidential records or records giving personal information: shred documents.
- Deletion of computer records.
- Transmission of records to an external body such as the County Records Office.

5.4 The following principles should be followed when disposing of records:

- All records containing personal or confidential information should be destroyed at the end of the retention period. Failure to do so could lead to the Council being prosecuted under the General Data Protection Regulations.
- the Freedom of Information Act or cause reputational damage.
- Where computer records are deleted steps should be taken to ensure that data is 'virtually impossible to retrieve' as advised by the Information Commissioner.
- Where documents are of historical interest it may be appropriate that they are transmitted to the County Records office.
- Back-up copies of documents should also be destroyed (including electronic or photographed documents unless specific provisions exist for their disposal).

5.5 Records should be maintained of appropriate disposals. These records should contain the following information:

- The name of the document destroyed.
- The date the document was destroyed.
- The method of disposal.

6. Data Protection Act 1998 – Obligation to Dispose of Certain Data

6.1 The Data Protection Act 1998 ('Fifth Principle') requires that personal information must not be retained longer than is necessary for the purpose for which it was originally obtained. Section 1 of the Data Protection Act defines personal information as:

Data that relates to a living individual who can be identified:

- a) from the data, or
- b) from those data and other information which is in the possession of, or is likely to come into the possession of the data controller.

It includes any expression of opinion about the individual and any indication of the intentions of the Council or other person in respect of the individual.

6.2 The Data Protection Act provides an exemption for information about identifiable living individuals that is held for research, statistical or historical purposes to be held indefinitely provided that the specific requirements are met.

6.3 Councils are responsible for ensuring that they comply with the principles of the under the General Data Protection Regulations namely:

- Personal data is processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.
- Personal data shall only be obtained for specific purposes and processed in a compatible manner.
- Personal data shall be adequate, relevant, but not excessive.
- Personal data shall be accurate and up to date.
- Personal data shall not be kept for longer than is necessary.
- Personal data shall be processed in accordance with the rights of the data subject.
- Personal data shall be kept secure.

6.4 External storage providers or archivists that are holding Council documents must also comply with the above principles of the General Data Protection Regulations.

7. Scanning of Documents

7.1 In general once a document has been scanned on to a document image system the original becomes redundant. There is no specific legislation covering the format for which local government records are retained following electronic storage, except for those prescribed by HM Revenue and Customs.

7.2 As a general rule hard copies of scanned documents should be retained for three months after scanning.

7.3 Original documents required for VAT and tax purposes should be retained for six years unless a shorter period has been agreed with HM Revenue and Customs.

8. Review of Document Retention

8.1 It is planned to review, update and where appropriate amend this document on a regular basis (at least every three years in accordance with the *Code of Practice on the Management of Records* issued by the Lord Chancellor).

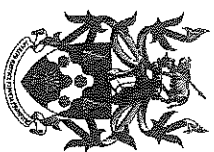
8.2 This document has been compiled from various sources of recommended best practice and with reference to the following documents and publications:

- *Local Council Administration*, Charles Arnold-Baker, 910^h edition, Chapter 11
- Local Government Act 1972, sections 225 – 229, section 234
- SLCC Advice Note 316 Retaining Important Documents
- SLCC Clerks' Manual: Storing Books and Documents
- *Lord Chancellor's Code of Practice on the Management of Records* issued under Section 46 of the *Freedom of Information Act 2000*

9. List of Documents

9.1 The full list of the Council's documents and the procedures for retention or disposal can be found in Appendix A: Inventory of Data captured, stored and processed by Bovey Tracey Town Council. This is updated regularly in accordance with any changes to legal requirements.

Bovey Tracey Town Council



Appendix A: List of Documents for Retention or Disposal

Document	Minimum Retention Period	Reason	Location Retained	Disposal
Minutes	Indefinite	Archive	Archive cupboard	Original signed paper copies of Council minutes of meetings must be kept indefinitely in safe storage. At regular intervals of not more than 5 years they must be archived and deposited with the Higher Authority
Agendas	5 years	Management	Open shelf	Bin (confidential waste shredded)
Accident/Incident reports	20 years	Potential claims	Filing cabinet	Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Scales of fees and charges	6 years	Management	Filing cabinet	Bin
Receipt and payment accounts	Indefinite	Archive	Filing cabinet	N/A
Receipt books of all kinds	6 years	VAT	Archive cupboard	Bin
Bank statements including	last completed audit year	Audit	Filing cabinet	Confidential waste

deposit/savings accounts					
Bank paying-in books	Last completed audit year	Audit	Safe	Confidential waste	
Cheque book stubs	Last completed audit year	Audit	Locked drawer	Confidential waste	
Quotations and tenders	6 years	Limitation Act 1980 (as amended)	Filing cabinet	Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.	
Paid invoices	6 years	VAT	Archive cupboard	Confidential waste	
Paid cheques	6 years	Limitation Act 1980 (as amended)	Archive cupboard	Confidential waste	
VAT records	6 years generally but 20 years for VAT on rents	VAT	Archive cupboard	Confidential waste	
Petty cash, postage and telephone books	6 years	Tax, VAT, Limitation Act 1980 (as amended)	Locked drawer	Confidential waste	
Timesheets	Last completed audit year 3 years	Audit (requirement) Personal Injury (best practice)	Filing cabinet	Bin	
Wages books/payroll	12 years	Superannuation	Filing cabinet	Confidential waste	
Insurance policies	While valid (but see next two items below)	Management	Filing cabinet	Bin	
Insurance company names and policy numbers	Indefinite	Management	Filing cabinet	N/A	
Certificates for insurance against liability for employees	40 years from date on which insurance commenced or was renewed	The Employers' Liability (Compulsory Insurance) Regulations 1998 (SI 2753) Management	On display	Bin	
Town Park equipment inspection reports	21 years		Filing cabinet	Confidential waste	
Investments	Indefinite	Audit, Management	N/A	N/A	

Title deeds, leases, agreements, contracts	Indefinite	Audit, Management	Safe	N/A
Members' allowances register	6 years	Tax, Limitation Act 1980 (as amended)	Filing cabinet	Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Information from other bodies e.g. circulars from county associations, NALC, principal authorities	Retained for as long as it is useful and relevant		Open shelf	Bin
Local/historical information	Indefinite – to be securely kept for benefit of the Parish	Councils may acquire records of local interest and accept gifts or records of general and local interest in order to promote the use for such records (defined as materials in written or other form setting out facts or events or otherwise recording information).	Filing cabinet/Archive Cupboard	N/A

Magazines and journals	Council may wish to keep its own publications For others retain for as long as they are useful and relevant.	The Legal Deposit Libraries Act 2003 (the 2003 Act) requires a local council which after 1 st February 2004 has published works in print (this includes a pamphlet, magazine or newspaper, a map, plan, chart or table) to deliver, at its own expense, a copy of them to the British Library Board (which manages and controls the British Library). Printed works as defined by the 2003 Act published by a local council therefore constitute materials which the British Library holds.	Open shelf	Bin if applicable
Record-keeping				
To ensure records are easily accessible it is necessary to comply with the following: <ul style="list-style-type: none"> • A list of files stored in cabinets will be kept • Electronic files will be saved using relevant file names 	The electronic files will be backed up periodically on a portable hard drive and also in the cloud-based programme supplied by the Council's IT company.	Management	Open shelf	Documentation no longer required will be disposed of, ensuring any confidential documents are destroyed as confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.

General correspondence	Unless it relates to specific categories outlined in the policy, correspondence, both paper and electronic, should be kept. Records should be kept for as long as they are needed for reference or accountability purposes, to comply with regulatory requirements or to protect legal and other rights and interests.	Management	Filing cabinet	Bin (shred confidential waste) A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
Correspondence relating to staff	If related to Audit, see relevant sections above. Should be kept securely and personal data in relation to staff should not be kept for longer than is necessary for the purpose it was held. Likely time limits for tribunal claims between 3–6 months. Recommend this period be for 3 years	After an employment relationship has ended, a council may need to retain and access staff records for former staff for the purpose of giving references, payment of tax, national insurance contributions and pensions, and in respect of any related legal claims made against the council.	Filing cabinet	Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.

		Documents from legal matters, negligence and other torts		
		<p>Most legal proceedings are governed by the Limitation Act 1980 (as amended). The 1980 Act provides that legal claims may not be commenced after a specified period. Where the limitation periods are longer than other periods specified the documentation should be kept for the longer period specified. Some types of legal proceedings may fall within two or more categories.</p> <p>If in doubt, keep for the longest of the three limitation periods.</p>		
Negligence	6 Years	Filing cabinet	Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.	
Defamation	1 year	Filing cabinet	Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.	
Contract	6 years	Safe	Confidential waste. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.	
Leases	12 years	Safe	Confidential waste.	
Sums recoverable by statute	6 years	Filing cabinet	Confidential waste.	
Personal injury	3 years	Filing cabinet	Confidential waste.	
To recover land	12 years	Filing cabinet	Confidential waste.	
Rent	6 years	Filing cabinet	Confidential waste.	
Breach of trust	None	Filing cabinet	Confidential waste.	
Trust deeds	Indefinite	Filing cabinet	N/A	
For Halls, Centres, Recreation Grounds				
<ul style="list-style-type: none"> • Application to hire • Invoices • Record of tickets issued 	6 years	VAT Filing cabinet	Confidential waste A list will be kept of those documents disposed of to	

Lettings diaries	Electronic files linked to accounts	VAT	Archive cupboard	meet the requirements of the GDPR regulations.
Terms and Conditions	6 years	Management	Filing cabinet	Bin
Event Monitoring Forms	6 years unless required for claims, insurance or legal purposes	Management	Filing cabinet	Bin. A list will be kept of those documents disposed of to meet the requirements of the GDPR regulations.
For Allotments				
Register and plans	Indefinite	Audit, Management	Filing cabinet	N/A
Minutes	Indefinite	Audit, Management	Filing cabinet	N/A
Legal papers	Indefinite	Audit, Management	Safe/Filing cabinet	N/A
For Burial Grounds				
<ul style="list-style-type: none"> • Register of fees collected • Register of burials • Register of purchased graves • Register/plan of grave spaces • Register of memorials • Applications for interment • Applications for right to erect memorials • Disposal certificates • Copy certificates of grant of exclusive right of burial 	Indefinite	Archives, Local Authorities Cemeteries Order 1977 (SI 204)	Filing cabinet	N/A

	Planning Papers		
Applications	1 year	Management	Bin
Appeals	1 year unless significant development	Management	Bin
Trees	1 year	Management	Bin
Local Development Plans	Retained as long as in force	Reference	Bin
Local Plans	Retained as long as in force	Reference	Bin
Town/Neighbourhood Plans	Indefinite – final adopted plans	Historical purposes	N/A
	CCTV		
Observation sheets	3 years	Data protection	Confidential waste
Internal Operations Procedure Manual	Destroy on renewal Review annually	Management	Confidential waste
Code of Practice	Destroy on renewal Review annually	Management	Confidential waste
Photographs/digital prints	31 days	Data protection	Confidential waste

Bovey Tracey Town Council

The Management of Transferable Data Policy



Contents

1	Purpose	2
2	Principals	2
3	Advice and Assistance	2
4	Responsibilities	3
5	Incident Management	3
6	Data Administration	3
7	Security	4
8	Use of removable media	4
9	Faulty or Unneeded Storage Devices	5
10	Breach procedures	5
11	Review And Revision	5
12	Employees Guide in Brief	5

Purpose

- 1.1 This policy supports the controlled storage and transfer of information by Councillors and all employees, temporary staff and agents (contractors, consultants and others working on behalf of the Council) who have access to and use of computing equipment that is owned or leased by Bovey Tracey Town Council.
- 1.2 Information is used throughout the Council and is sometimes shared with external organisations and applicants. The use of removable media may result in the loss of the ability to access information, or interference with the integrity of information, which could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide services to the public.
- 1.3 It is therefore essential for the continued operation of the Council that the availability, integrity and confidentiality of all storage devices are maintained at a level which is appropriate to the Council's needs.
- 1.4 The aims of the policy are to ensure that the use of removable storage devices is accomplished with due regard to:
 - 1.4.1 Enabling the correct data to be made available where it is required
 - 1.4.2 Maintaining the integrity of the data
 - 1.4.3 Preventing unintended consequences to the stability of the computer network
 - 1.4.4 Building confidence and trust in data that is being shared between systems
 - 1.4.5 Maintaining high standards of care towards data and information about individual parishioners, staff or information that is exempt from disclosure
 - 1.4.6 Compliance with legislation, policies or good practice requirements

2 Principals

- 2.1 This policy sets out the principles that will be adopted by the Council in order for material to be safely stored on removable media so that the risk of loss or corruption to work data is low.
- 2.2 Removable media includes but is not limited to:
USB memory sticks, memory cards, portable memory devices, CD / DVDs, diskettes and any other device that transfers data between systems, or stores electronic data separately from email or other applications.
- 2.4 Any person who intends to store Council data on removable media must abide by this Policy. This requirement devolves to Councillors, employees and agents of the Council, who may be held personally liable for any breach of the requirements of this policy.
- 2.5 Failure to comply with this policy could result in disciplinary action.

3 Advice and Assistance

- 3.1 The clerk will ensure that everyone that is authorised to access the Councils information systems is aware of their obligations arising from this policy.

- 3.2 A competent person should be consulted over any hardware or system issues. Advice and guidance on using software packages should be also sort from a competent person.

4 **Responsibilities**

- 4.1 Clerks are responsible for enforcing this policy and for having arrangements in place to identify the location of all data used in connection with Council business.
- 4.2 Users of removable media must have adequate Records Management / Information Security training so that relevant policies are implemented.

5 **Incident Management**

- 5.1 It is the duty of all employees and agents of the Council to not allow storage media to be compromised in any way whilst in their care or under their control. There must be immediate reporting of any misuse or irresponsible actions that affect work data or information, any loss of material, or actual, or suspected breaches in information security to the clerk.
- 5.2 It is the duty of all Councillors/Employees to report any actual or suspected breaches in information security to the clerk.

6 **Data Administration**

- 6.1 Removable media should not be the only place where data created or obtained for work purposes is held, as data that is only held in one place and in one format is at much higher risk of being unavailable through loss, destruction or malfunction of equipment, than data which is routinely backed up.
- 6.2 Where removable media is used to transfer material between systems then copies of the data should also remain on the source system or computer, until the data is successfully transferred to another computer or system.
- 6.3 Where there is a business requirement to distribute information to third parties, then removable media must only be used when the file cannot be sent or is too large to be sent by email or other secure electronic means.
- 6.4 Transferring material to removable media is a snapshot of the data at the time it was saved to the media. Adequate labelling must be undertaken so as to easily identify the version of the data, as well as its content.
- 6.5 Files must be deleted from removable media, or the removable media destroyed, when the operational use of the material has been completed. The Council's retention and disposition schedule must be implemented by Councillors, employees, contractors and agents for all removable media.

7 Security

- 7.1 All storage media must be kept in an appropriately secure and safe environment that avoids physical risk, loss or electrical corruption of the business asset. Due to their small size there is a high risk of the removable media being mislaid lost or damaged, therefore special care is required to physically protect the device and the data. Anyone using removable media to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- 7.2 Virus Infections must be prevented from damaging the Councils network and computers. Virus and malware checking software approved by the Council, must be operational on both the machine from which the data is taken and the machine on to which the data is to be loaded. The data must be scanned by the virus checking software, before the media is loaded on to the receiving machine.
- 7.3 Any memory stick used in connection with Council equipment or to store Council material should usually be Council owned. However, work related data from external sources can be transferred to the Council network using memory sticks that are from trusted sources and have been checked using current anti-virus software.
- 7.4 The Council will not provide support or administrator access for any non-council memory stick.

8 Use of removable media

- 8.1 Care must be taken over what data or information is transferred onto removable media. Only the data that is authorised and necessary to be transferred should be saved on to the device.
- 8.3 Council material belongs to the Council and any equipment on which it is held should be under the control of the Council and not available to be used for other purposes that may compromise the data.
- 8.4 All data transferred to removable media should be in accordance with an agreed process established by the Council so that material can be traced.
- 8.5 The person arranging the transfer of data must be authorised to make use of, or process that particular data.
- 8.6 Whilst in transit or storage the data must be given appropriate security according to the type of data and its sensitivity.
- 8.7 Encryption must be applied to the data file unless there is no risk to the Council, other organisations or individuals from the data being lost whilst in transit or storage. If encryption is not available then password control must be applied if removable media must be used for the business purpose.

9 Faulty or Unneeded Storage Devices

- 9.1 Damaged or faulty media must not be used. The clerk must be consulted over any damaged equipment, peripherals or media.
- 9.2 All unneeded or faulty storage devices must be dealt with securely to remove the data before reallocating or disposing of the device.

10 Breach procedures

- 10.1 Users who do not adhere to this policy will be dealt with through the Councils disciplinary process.
- 10.2 Where external service providers, agents or contractors breach the policy, this should be addressed through contract arrangements.

11 Review and Revision

- 11.1 This policy will be reviewed annually by the Council and revised according to developments in legislation, guidance, accepted good practice and operational use.

12 Employees Guide in Brief

- 12.1 Data and information are valuable and must be protected.
- 12.2 Only transfer data onto removable media, if you have the authority to do so.
- 12.4 All transfer arrangements carry a risk to the data.
- 12.5 Run the virus checking programme on the removable media each time it is connected to a computer.
- 12.6 Only use approved products for Council data.
- 12.7 Activate encryption on removable media wherever it is available and password protection if not available
- 12.8 Data should be available for automatic back up and not solely saved to removable media.
- 12.9 Delete files from removable media, or destroy the media, after the material has been used for its purpose.

Bovey Tracey Town Council



Social Media and Electronic Communication Policy

The use of digital and social media and electronic communication enables the Town Council to interact in a way that improves the communications both within the Council and between the Council and the people, businesses and agencies it works with and serves.

The Council has a website, Facebook page, Twitter account and uses email to communicate. The Council will always try to use the most effective channel for its communications. Over time the Council may add to the channels of communication that it uses as it seeks to improve and expand the services it delivers. When these changes occur, this Policy will be updated to reflect the new arrangements.

The Council Facebook pages and Twitter account intends to provide information and updates regarding activities and opportunities within our Parish/Town and promote our community positively.

Communications from the Council will meet the following criteria:

- Be civil, tasteful and relevant;
- Not contain content that is knowingly unlawful, libellous, harassing, defamatory, abusive, threatening, harmful, obscene, profane, sexually oriented or racially offensive;
- Not contain content knowingly copied from elsewhere, for which we do not own the copyright;
- Not contain any personal information.
- If it is official Council business it will be moderated by either the Chair/Vice Chair of the Council or the Clerk to the Council;
- Social media will not be used for the dissemination of any political advertising.

In order to ensure that all discussions on the Council page are productive, respectful and consistent with the Council's aims and objectives, we ask you to follow these guidelines:

- Be considerate and respectful of others. Vulgarity, threats or abuse of language will not be tolerated.
- Differing opinions and discussion of diverse ideas are encouraged, but personal attacks on anyone, including the Council members or staff, will not be permitted.
- Share freely and be generous with official Council posts, but be aware of copyright laws; be accurate and give credit where credit is due.
- Stay on topic.

- Refrain from using the Council's Facebook page or Twitter site for commercial purposes or to advertise market or sell products.

The site is not monitored 24/7 and we will not always be able to reply individually to all messages or comments received. However, we will endeavour to ensure that any emerging themes or helpful suggestions are passed to the relevant people or authorities. Please do not include personal/private information in your social media posts to us.

Sending a message/post via Facebook or Twitter will not be considered as contacting the Council for official purposes and we will not be obliged to monitor or respond to requests for information through these channels. Instead, please make direct contact with the council's Clerk and/or members of the council by emailing.

We retain the right to remove comments or content that includes:

- Obscene or racist content
- Personal attacks, insults, or threatening language
- Potentially libellous statements.
- Plagiarised material; any material in violation of any laws, including copyright
- Private, personal information published without consent
- Information or links unrelated to the content of the forum
- Commercial promotions or spam
- Alleges a breach of a Council's policy or the law

The Council's response to any communication received not meeting the above criteria will be to either ignore, inform the sender of our policy or send a brief response as appropriate. This will be at the Council's discretion based on the message received, given our limited resources available. Any information posted on the Facebook page not in line with the above criteria will be removed as quickly as practically possible. Repeat offenders will be blocked from the Facebook page. The Council may post a statement that '*A post breaching the Council's Social Media Policy has been removed*'. If the post alleges a breach of a Council's policy or the law the person who posted it will be asked to submit a formal complaint to the Council or report the matter to the Police as soon as possible to allow due process.

Town Council Website

Where necessary, we may direct those contacting us to our website to see the required information, or we may forward their question to one of our Councillors for consideration and response. We may not respond to every comment we receive particularly if we are experiencing a heavy workload.

The Council may, at its discretion, allow and enable approved local groups to have and maintain a presence on its website for the purpose of presenting information about the group's activities. The local group would be responsible for maintaining the content and ensuring that it meets the Council's 'rules and expectation' for the web site. The Council reserves the right to remove any or all of a local group's information from the web site if it

feels that the content does not meet the Council's 'rules and expectation' for its website. Where content on the website is maintained by a local group it should be clearly marked that such content is not the direct responsibility of the Council.

Parish/Town Council email

The Clerk to the council has their own council email address (info@boveytracey.gov.uk) The email account is monitored mainly during office hours, Monday to Friday, and we aim to reply to all questions sent as soon as we can. An 'out of office' message is used when appropriate.

The Clerk is responsible for dealing with email received and passing on any relevant mail to members or external agencies for information and/or action. All communications on behalf of the Council will usually come from the Clerk, and/or otherwise will always be copied to the Clerk. All new Emails requiring data to be passed on, will be followed up with a Data consent form for completion before action is taken with that correspondence.

Individual Councillors are at liberty to communicate directly with parishioners in relation to their own personal views, if appropriate, copy to the Clerk. NB any emails copied to the Clerk become official and will be subject to The Freedom of Information Act. These procedures will ensure that a complete and proper record of all correspondence is kept.

Do not forward personal information on to other people or groups outside of the Council, this includes names, addresses, email, IP addresses and cookie identifiers.

SMS (texting)

Members and the Clerk may use SMS as a convenient way to communicate at times. All are reminded that this policy also applies to such messages.

Video Conferencing e.g. Skype

If this medium is used to communicate please note that this policy also applies to the use of video conferencing.

Internal communication and access to information within the Council

The Council is continually looking at ways to improve its working and the use of social media and electronic communications is a major factor in delivering improvement.

Councillors are expected to abide by the Code of Conduct and the Data Protection Act in all their work on behalf of the Council

As more and more information becomes available at the press of a button, it is vital that all information is treated sensitively and securely. Councillors are expected to maintain an awareness of the confidentiality of information that they have access to and not to share confidential information with anyone. Failure to properly observe confidentiality may be seen as a breach of the Council's Code of Conduct and will be dealt with through its prescribed procedures (at the extreme it may also involve a criminal investigation).

Members should also be careful only to cc essential recipients on emails i.e. to avoid use of the 'Reply to All' option if at all possible, but of course copying in all who need to know and ensuring that email trails have been removed.

DRAFT



PRIVACY NOTICE - GENERAL

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 Bovey Tracey 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

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

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

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

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

- Where you pay for activities such as use of a council hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- The personal data we process may include sensitive or other special categories of personal data such as criminal convictions, racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sexual life or orientation.

How we use sensitive personal data

- We may process sensitive personal data including, as appropriate:
 - information about your physical or mental health or condition (employees) 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 etc);
- To help us to build up a picture of how we are performing;
- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions;
- To enable us to meet all legal and statutory obligations and powers including any delegated functions;
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury;
- To promote the interests of the council;
- To maintain our own accounts and records;
- To seek your views, opinions or comments;
- To notify you of changes to our facilities, services, events and staff, councillors and other role holders;
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives;
- To process relevant financial transactions including grants and payments for goods and services supplied to the council
- To allow the statistical analysis of data so we can plan the provision of services.

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

What is the legal basis for processing your personal data?

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

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

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

Sharing your personal data

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

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

How long do we keep your personal data?

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

Your rights and your personal data

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

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

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

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

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

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

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

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

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

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

5) *The right to data portability*

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

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

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

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

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

Transfer of Data Abroad

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

Further processing

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

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on this web page www.boveytracey.gov.uk. This Notice was last updated in April 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 to:

The Data Controller, The Town Clerk, Bovey Tracey Town Council, Town Hall, Town Hall Place, Bovey Tracey, TQ13 9EG. Email: info@boveytracey.gov.uk.



SUBJECT ACCESS REQUESTS POLICY

What is a Subject Access Request (SAR)?

This right, commonly referred to as subject access request, is created by section 7 of the Data Protection Act. It is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this, and an individual who makes a written request is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people,
- given a copy of the information comprising the data; and given details of the source of the data (where this is available).

In most cases you must respond to a subject access request promptly and in any event within 40 calendar days of receiving it. However, some types of personal data are exempt from the right of subject access and so cannot be obtained by making a subject access request.

1. Upon receipt of a SAR

- (a) Verify whether you are controller of the data subject's personal data. If you are not a controller, but merely a processor, inform the data subject and refer them to the actual controller.
- (b) Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.
- (c) Verify the access request; is it sufficiently substantiated? Is it clear to the data controller what personal data is requested? If not: request additional information.
- (d) Verify whether requests are unfounded or excessive (in particular because of their repetitive character); if so, you may refuse to act on the request or charge a reasonable fee.
- (e) Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR.
- (f) Verify whether you process the data requested. If you do not process any data, inform the data subject accordingly. At all times make sure the internal SAR policy is followed and progress can be monitored.
- (g) Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.
- (h) Verify whether the data requested also involves data on other data subjects and make sure this data is filtered before the requested data is supplied to the data subject; if data cannot be filtered, ensure that other data subjects have consented to the supply of their data as part of the SAR.

2. Responding to a SAR

- (a) Respond to a SAR within one month after receipt of the request:
 - (i) If more time is needed to respond to complex requests, an extension of another two months is permissible, provided this is communicated to the data subject in a timely manner within the first month;
 - (ii) if the council cannot provide the information requested, it should inform the data subject on this decision without delay and at the latest within one month of receipt of the request.
- (b) If a SAR is submitted in electronic form, any personal data should preferably be provided by electronic means as well.
- (c) If data on the data subject is processed, make sure to include as a minimum the following information in the SAR response:
 - (i) the purposes of the processing;
 - (ii) the categories of personal data concerned;
 - (iii) the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules¹ or EU model clauses²;
 - (iv) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
 - (v) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
 - (vi) the right to lodge a complaint with the Information Commissioners Office ("ICO");
 - (vii) if the data has not been collected from the data subject: the source of such data;
 - (viii) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- (d) Provide a copy of the personal data undergoing processing.

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

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

What must I do?

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

How must I do it?

1. Notify the Town Clerk upon receipt of a request
2. We must ensure a request has been received in writing where a data subject is asking for sufficiently well-defined personal data held by the council relating to the data subject. You should clarify with the requestor what personal data they need. They must supply their address and valid evidence to prove their identity. The council accepts the following forms of identification (* These documents must be dated in the past 12 months, +These documents must be dated in the past 3 months):
 - Current UK/EEA Passport
 - UK Photocard Driving Licence (Full or Provisional)
 - Firearms Licence / Shotgun Certificate
 - EEA National Identity Card
 - Full UK Paper Driving Licence
 - State Benefits Entitlement Document*
 - State Pension Entitlement Document*
 - HMRC Tax Credit Document*
 - Local Authority Benefit Document*
 - State/Local Authority Educational Grant Document*
 - HMRC Tax Notification Document
 - Disabled Driver's Pass
 - Financial Statement issued by bank, building society or credit card company+

- Judiciary Document such as a Notice of Hearing, Summons or Court Order
 - Utility bill for supply of gas, electric, water or telephone landline+
 - Most recent Mortgage Statement
 - Most recent council Tax Bill/Demand or Statement
 - Tenancy Agreement
 - Building Society Passbook which shows a transaction in the last 3 months and your address
3. Depending on the degree to which personal data is organised and structured, you will need to search emails (including archived emails and those that have been deleted but are still recoverable), Word documents, spreadsheets, databases, systems, removable media (for example, memory sticks, floppy disks, CDs), tape recordings, paper records in relevant filing systems etc. which your area is responsible for or owns.
 4. You must not withhold personal data because you believe it will be misunderstood; instead, you should provide an explanation with the personal data. You must provide the personal data in an "intelligible form", which includes giving an explanation of any codes, acronyms and complex terms. The personal data must be supplied in a permanent form except where the person agrees or where it is impossible or would involve undue effort. You may be able to agree with the requester that they will view the personal data on screen or inspect files on our premises. You must redact any exempt personal data from the released documents and explain why that personal data is being withheld.
 5. Make this clear on forms and on the council website
 6. You should do this through the use of induction, my performance and training, as well as through establishing and maintaining appropriate day to day working practices.
 7. A database is maintained allowing the council to report on the volume of requests and compliance against the statutory timescale.
 8. When responding to a complaint, we must advise the requestor that they may complain to the Information Commissioners Office ("ICO") if they remain unhappy with the outcome.

Bovey Tracey Town Council



Subject Access Request (SAR) Form

Process to Action		
Name of requester:		
(Method of communication):		
Email Address:		
Phone number:		
Postal Address:		
Date Subject Access Request made		
Is the request made under the Data Protection Legislation	Yes	No
Date Subject Access Request action to be completed by (One month after receipt time limit)		
Extension to the date of reply requested (An extension of another two months is permissible provided it is communicated to the subject within the one month period)	Yes	No
Extension date advised to the Subject Requester and method of contact		
Identification must be proven from the below list: Current UK/EEA Passport UK Photo card Driving Licence (Full or Provisional) EEA National Identity Card Full UK Paper Driving Licence State Benefits Entitlement Document State Pension Entitlement Document HMRC Tax Credit Document Local Authority Benefit Document State/Local Authority Educational Grant Document HMRC Tax Notification Document Disabled Driver's Pass Financial Statement issued by bank, building society or credit card company Utility bill for supply of gas, electric, water or telephone landline A recent Mortgage Statement A recent council Tax Bill/Demand or Statement Tenancy Agreement Building Society Passbook which shows a transaction in the last 3 months and their address		
Verification sought that the Subject Access request is substantiated	Yes	No
Verification received	Yes	No
Verification if the Council cannot provide the information requested	Yes	No
Is the request excessive or unfounded?	Yes	No
Request to be actioned	Yes	No
Fee to be charged (Subject Access requests must be undertaken free of charge to a requester unless the legislation permits a reasonable charge)	Yes	No
If the request is to be refused, action to be taken and by whom.		

Changes requested to data/ or removal	
Complaint Process (Where a requestor is not satisfied with a response to a SAR, the council must manage this as a complaint)	
Completion date of request	
Date complaint received by requested and details of the complaint	
Date complaint completed and outcome	

Categories of Data to Check

Data	Filing Cabinet	Laptop	Checked	Corrected/Deleted	Actioned by
HR					
Democracy					
Statutory Function					
Legal					
Business					
Legal requirement					
General Data					
Consultation Data					

Bovey Tracey Town Council



Data Security Breach Reporting Form

A data security breach can happen for a number of reasons: Loss or theft of data or equipment on which data is Stored, Inappropriate access controls allowing unauthorised use, Equipment failure, Human error, Unforeseen circumstances such as a fire or flood, Hacking attack, 'Blagging' offences where information is obtained by deceiving the organisation who holds it. Use this form to report such breaches.

Example: Reportable Theft or loss of an unencrypted laptop computer or other unencrypted portable electronic/digital media holding names, addresses, dates of birth and National Insurance Numbers of individuals. A manual paper-based filing system (or unencrypted digital media) holding the personal data relating to named individuals and their financial records etc. More information can be found using the below link:

<https://ico.org.uk/media/for-organisations/documents/1562/guidance-on-data-security-breach-management.pdf>

Breach Containment and Recovery

Article 2(2) of the Notification Regulation states:

The provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible. The provider shall include in its notification to the competent national authority the information set out in Annex I. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) provide rules about sending marketing and advertising by electronic means, such as by telephone, fax, email, text and picture or video message, or by using an automated calling system. PECR also include other rules relating to cookies, telephone directories, traffic data, location data and security breaches. Detection of a personal data breach shall be deemed to have taken place when the provider has acquired sufficient awareness that a security incident has occurred that led to personal data being compromised, in order to make a meaningful notification as required under this Regulation.

Date and time of Notification of Breach	
Notification of Breach to whom Name Contact Details	
Details of Breach	

Nature and content of Data Involved	
Number of individuals affected:	
Name of person investigating breach Name Job Title Contact details Email Phone number Address	
Information Commissioner informed Time and method of contact https://report.ico.org.uk/security-breach/	
Police Informed if relevant Time and method of contact Name of person contacted Contact details	
Individuals contacted How many individuals contacted? Method of contact used to contact? Does the breach affect individuals in other EU member states? What are the potential consequences and adverse effects on those individuals? Confirm that details of the nature of the risk to the individuals affected: any measures they can take to safeguard against it; and the likely cost to them of	

taking those measures is relayed to the individuals involved.	
Staff briefed	
Assessment of ongoing risk	
Containment Actions: technical and organisational security measures have you applied (or were to be applied) to the affected personal data	
Recovery Plan	
Evaluation and response	

Bovey Tracey Town Council

CONSENT FORM



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

If you are aged 13 or under your parent or guardian should fill in their details below to confirm their consent

Name
.....

Address
.....
.....
.....

Email
.....

Signature

Date

Please confirm your consent below. You can grant consent to any or all of the purposes listed. You can find out more about how we use your data from our "Privacy Notice" which is available from our website (www.boveytracey.gov.uk) or from the Town Council Office.

You can withdraw or change your consent at any time by contacting the Town Council Office.

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

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

- We may use your name and photo in our newsletters, bulletins or on our website, or our social media accounts (for example our Facebook page or Twitter account).
- Other specific additional activities, not included in the above to be listed here.

Keeping in touch:

- Yes please, I would like to receive communications by email
- Yes please, I would like to receive communications by telephone
- Yes please, I would like to receive communications by mobile phone including text message
- Yes please, I would like to receive communications by social media (for example Facebook, Twitter etc)
- Yes please, I would like to receive communications by post

Section 1 – Annual Governance Statement 2017/18

We acknowledge as the members of:

ENTER NAME OF AUTHORITY

our responsibility for ensuring that there is a sound system of internal control, including arrangements for the preparation of the Accounting Statements. We confirm, to the best of our knowledge and belief, with respect to the Accounting Statements for the year ended 31 March 2018, that:

	Agreed		'Yes' means that this authority:
	Yes	No*	
1. We have put in place arrangements for effective financial management during the year, and for the preparation of the accounting statements.			<i>prepared its accounting statements in accordance with the Accounts and Audit Regulations.</i>
2. We maintained an adequate system of internal control including measures designed to prevent and detect fraud and corruption and reviewed its effectiveness.			<i>made proper arrangements and accepted responsibility for safeguarding the public money and resources in its charge.</i>
3. We took all reasonable steps to assure ourselves that there are no matters of actual or potential non-compliance with laws, regulations and Proper Practices that could have a significant financial effect on the ability of this authority to conduct its business or manage its finances.			<i>has only done what it has the legal power to do and has complied with Proper Practices in doing so.</i>
4. We provided proper opportunity during the year for the exercise of electors' rights in accordance with the requirements of the Accounts and Audit Regulations.			<i>during the year gave all persons interested the opportunity to inspect and ask questions about this authority's accounts.</i>
5. We carried out an assessment of the risks facing this authority and took appropriate steps to manage those risks, including the introduction of internal controls and/or external insurance cover where required.			<i>considered and documented the financial and other risks it faces and dealt with them properly.</i>
6. We maintained throughout the year an adequate and effective system of internal audit of the accounting records and control systems.			<i>arranged for a competent person, independent of the financial controls and procedures, to give an objective view on whether internal controls meet the needs of this smaller authority.</i>
7. We took appropriate action on all matters raised in reports from internal and external audit.			<i>responded to matters brought to its attention by internal and external audit.</i>
8. We considered whether any litigation, liabilities or commitments, events or transactions, occurring either during or after the year-end, have a financial impact on this authority and, where appropriate, have included them in the accounting statements.			<i>disclosed everything it should have about its business activity during the year including events taking place after the year end if relevant.</i>
9. (For local councils only) Trust funds including charitable. In our capacity as the sole managing trustee we discharged our accountability responsibilities for the fund(s)/assets, including financial reporting and, if required, independent examination or audit.	Yes	No	N/A

*Please provide explanations to the external auditor on a separate sheet for each 'No' response. Describe how the authority will address the weaknesses identified.

This Annual Governance Statement is approved by this authority and recorded as minute reference:

MINUTE REFERENCE
dated DD/MM/YY

Signed by the Chairman and Clerk of the meeting where approval is given:

Chairman SIGNATURE REQUIRED
Clerk SIGNATURE REQUIRED

Other information required by the Transparency Codes (not part of Annual Governance Statement)
Authority web address

AUTHORITY WEBSITE ADDRESS