WTCAM 31/05/2018

Item 14

GENERAL DATA PROTECTION REGULATIONS

Purpose of the Report and Recommendation

To report on the provisions of the General Data Protection Regulations and to seek Council's approval of the recommendations shown at 2.1, 2.2, 2.3 and 2.4

1.0 INTRODUCTION

1.1 The General Data Protection Regulations (GDPR) will come into force on 25th May 2018 and will significantly increase the legal responsibilities placed on the Council as the organisation which controls and processes personal data and also increases the rights of individuals to challenge the accuracy of data councils hold

1.2 There was a very informative training course for Councillors on GDPR given by CBC on 6th April 2018 where details of the Regulations were discussed.

1.3 Attached for members' consideration/information is a report on the provisions of GDPR together with draft documents to go on the Council's website. These policies/documents were produced by NALC and Winkworth Sherwood, Solicitors and Parliamentary Agents.

1.4 Although the Regulations come into force on 25th May 2018 the ICO have said that they want to work with organisations to make sure they are compliant, not to punish them.

2.0 RECOMMENDATION

2.1 To note the implications of and work undertaken for the preparation of GDPR contained in the attached report

2.2 That the draft policies and documents shown at Appendix 1 of the report be approved and put on the Council's website

2.3 That the Council appoint CBC Information Officer as its DPO

2.4 That monthly reports be given to the Council on GDRP compliance/progress

General Data Protection Regulations (GDPR) 2018

Introduction

The new General Data Protection Regulation (GDPR) replaces the 1998 Data Protection Act (DPA) and gives individuals more rights and protection regarding how their personal data is used by councils. It contains 99 Articles and Local Councils must comply with its requirements. The introduction of the new legislation is not affected by Brexit.

GDPR retains the existing legal principles of the Data Protection Act 1998 (DPA) but updates it to take into account digital technology and current global working practices. One of the main changes is that GDPR places a much greater emphasis on transparency, openness and the documents the Council needs to keep to show that it is complying with the legislation.

In essence GDPR:-

- Increases the legal responsibilities placed on the Council as the organisation which controls personal data known as "the data controller" as well as on the Council's providers known as "data processors" and

- Increases the rights of individuals whose data is entrusted to the Council (known as "data subjects") to challenge the accuracy of the data the Council holds and even, in some situations to require the Council to delete their personal data

The Information Commissioner (ICO) who is the regulator of GDPR intends to provide further guidance on this and this will be reported to Council.

Guidance has been produced by the ICO and this is Guide to General Data Protection Regulation (GDPR) ICO and is available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdrp/

Personal Data

GDPR applies only to personal data that is data about an identifiable **living** individual who can be identified from that data. A name on its own may not be sufficient to be personal data but if the Council holds any other information that can be linked to the name then that would make it personal data.

The GDRP gives a framework for the treatment of personal data with problems most likely to occur through social media because as soon as anything has been opened it has been processed and once it has been processed it can't be unprocessed.

Core Principles of GDPR

The six core principles of GDPR (Article 5 of the Regulations) relating to personal data can be summarised as follows

(a) Must be processed lawfully, fairly and transparently.

(b) Is only used for a specific processing purpose that the data subject has been made aware of and no other, without further consent.

(c) Should be **adequate, relevant and limited** to what is necessary i.e. only the minimum amount of data should be kept for specific processing.

(d) Must be **accurate** and where necessary **kept up to date**. Every reasonable step must be taken to ensure that personal data that is inaccurate having regard to the purpose for which it is processed is erased or rectified without delay.

(e) Kept in a form which permits identification of data subjects Should **not be stored for longer than is necessary**, and that storage is safe and secure.

(f) Should be processed in a manner that ensures **appropriate security and protection** including protection against unauthorised or unlawful processing and against accidental loss destruction or damage.

All organisations have to comply with GDPR and it is regulated by the ICO and the ICO has produced a 12 step guide to assist organisations in working towards compliance as shown below.

Checklist Item	Actions Taken	Achieved
Awareness	Decision makers and key people should be made aware of the changes in legislation	There has been training
Information held	Document all personal data held, where it comes from and whom it is shared with.	Prepared in draft form
Communicating privacy information	Review current privacy notices and put plan in place to make necessary changes.	Prepared in draft form
Individuals rights	Review procedures to ensure they cover the rights individuals have.	In progress
Subject Access Requests	Update procedures and plan how to handle future requests	Prepared in draft form
Lawful basis for processing personal data	Identify lawful basis for processing activities.	In progress
Consent	Review how consent is sought, recorded and managed and identify changes required.	In progress
Children	Consider whether you need to put systems in place to verify individual's ages and to obtain parental or guardian consent for data processing activity.	In progress
Data breaches	Procedure to detect, report and investigate a personal data breach	In progress

Data Protection by Design and Data Protection Impact Assessments	Legal requirement. DPIAs are now mandatory in certain circumstances. Processes and policies need to be put in place.	In progress
Data Protection Officers	Designate a DPO (ensure there is no conflict of interest)Not necessary for small parish councils but may be best practice for large parish councils	In progress But may not be required
International	WTC does not carry out cross-border processing and needs take no further action.	N/A

Personal Data

GDPR applies only to personal data that is data about an identifiable **living** individual who can be identified from that data. A name on its own may not be sufficient to be personal data but if the Council holds any other information that can be linked to the name then that would make it personal data.

The GDPR gives a framework for the treatment of personal data with problems most likely to occur through social media because as soon as anything has been opened it has been processed and once it has been processed it can't be unprocessed.

If personal data is collected, used or stored on behalf of the Council then the first thing is to consider and be sure about is that there is a lawful reason for holding and dealing with the data. There are six reasons set out in GDPR (Article 6) but only the first four are likely to apply to Council data:-

- Contract obligation – The Council needs to use (or "process") the data for a contract that the Council has with an individual
- Legal obligation – The Council needs to use the data so that it can comply with the law
- Public interest – It is necessary to use the information for a task that is in the public interest or for an official function. This will cover anything that the Council must do in the public interest but not things it would like to do
- Consent – If the individual has given clear consent. But consent should only be asked for if none of the other reason above apply.
- Legitimate interests
- Vital interests – matter of life and death

Once the lawful basis for processing the data has been ascertained the second thing that needs to be considered is whether the processing is necessary. Use or processing of the data is necessary if it is reasonably needed to carry out what the council needs the data for. For example the lawful basis for processing the personal data in a planning application is "compliance with a legal obligation".

Sensitive Personal Data (Article 9)

This is a special kind of personal data which because of its nature is especially confidential and to which stricter rules apply (see below). In the legislation it is known as "special categories of personal data" and these are listed in the GDPR and the most important categories are as follows:-

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs, or
- Trade union membership
- The processing of genetic data, biometric data for the purpose of uniquely identifying a natural person of the data subject has been obtained
- Data concerning health
- Data concerning a person's sex life or sexual orientation

The processing of special categories of personal data is prohibited subject to the exceptions stated in Article 9. As stated in the previous paragraph Data Controllers need to establish a lawful basis for processing and if sensitive personal information is being processed it must be established that at least one of the criteria listed below applies:-

- Explicit consent – of the data subject has been obtained
- Employment Law – if necessary for employment law
- Vital Interests – in a life or death situation
- Charities, Religious organisations or not for profit organisations – to further the interests of the organisation on behalf of members, former members
- Data made public by the data subject – the data must have been made public manifestly
- Legal claims – where necessary for the establishment, exercise or defence of legal claims or for the Courts acting in this judicial capacity

- Reasons of substantial public interest – where proportionate to the aim pursued and the rights of individuals are protected

- Medical diagnosis or treatment – where necessary for medical treatment by health professionals including assessing work capacity or the management of health and social care systems

- Public Health – where necessary for reasons of public health

- Historical, statistical or scientific purposes – where necessary for statistical purposes in the public interest for historical, scientific research or statistical purposes

In a Council context the most relevant lawful basis for processing under Special Category basis are likely to be explicit consent; employment law or Reasons of substantial public interest.

Processing Personal Data about Children

Under GDPR parental consent will be required for the processing of personal data of children under 16. European Member states may lower the age requiring parental consent to 13. The Data protection Bill has adopted this option to reduce the age of consent to 13 but this is subject to parliamentary approval.

GDPR - What's New?

- New duty to appoint a Data Protection Officer (DPO). However on 9th May 2018 during the report and remaining stages of the Data Protection Bill MPs accepted the Government's amendment to exempt all parish and town councils from the requirement to appoint a DPO under GDPR. This Bill now enters the House of Lords who will consider the amendments made in the House of Commons although it is not expected that this particular amendment will be reversed. It is expected that the Bill will come into force by 25th May 2018.The Data Protection Bill updates data protection in the UK, supplementing the GDPR and implementing the EU law. The Government will produce guidance on this when it becomes law.

  Notwithstanding that there may not be a legal requirement for parish and town councils to appoint a DPO because this Council is a larger Town Council it is considered that it would be best practice to appoint a DPO.

- The DPO is a mandatory appointment and must be made on the basis of appropriate professional qualities having an expert knowledge of data protection law and there is a school of thought that says the DPO should also be independent.

The Council has approached Copeland Borough Council (as have other town councils) to ask if it would be possible for their Information Management Officer to take on the role as DPO for the Town Council and a reply is awaited.

- New approach to relying on consent for processing personal data.
- New duty to report data breaches (including to the ICO). Every breach has to be reported within 72 hours of discovery. The fine rate is approximately £1,000 per letter going astray with personal details on it.
- Responding to subject access requests – within 1 calendar month and cannot charge However Councils will be able to refuse or charge a reasonable fee
- More rights for individuals:-
    - The right of access – individuals will be able to access their data to verify the lawfulness of the processing and this will be by subject access requests
    - The right to rectification. This right arises in the event of inaccurate or incomplete data (Article 16)
    - The right to erasure (the "right to be forgotten) (Article 17)
    - The right to restriction of processing (Article 18)
    - The notification obligation regarding rectification or erasure of personal data or restriction of processing (Article 19)
    - The right to data portability. This enables individuals to reuse and transfer their personal data (held in electronic form) for their personal use to another data controller without restriction as to its usability. (Article 20)
    - The right to object and automated decision making (Article 21)
- New duty to keep an internal register of processing activities
- Need for privacy notices
- Privacy impact assessments in respect of activities to be determined by the ICO – ie when considering using CCTV
- Robust contracts between data controllers (councils) and data processors
- New fines coming in (though there are many stages - warnings, reprimands, corrective orders - before the ICO would fine a data controller or processor).

The ICO will be able to impose fines of up to €20,000,000 or 4% of annual turnover of an organisation for personal data breaches

What Does it Mean for Local Councils?

Virtually all local councils collect and hold personal information on their members, staff, residents, contractors etc, so it is important to be prepared for the introduction of GDPR. **The Information Commissioner's Office (ICO) recognises that not all organisations will be fully GDPR-compliant by May 2018, but will expect to see strong evidence that any organisation that comes to its attention is taking action to meet GDPR requirements.** This means being able to:

- Demonstrate what work an organisation has done to prepare for and comply with GDPR
- Outline what has yet to be done, when it will be done and by whom.

Enforcement of GDRP

The ICO will police the GDPR and there are 4 levels of sanctions for personal data breaches:-

1. That steps must be taken to improve

2. An Enforcement Notice is served stating that specific steps must be taken and that the specific processing must stop. Breach of an Enforcement Notice is a criminal offence.

3. Monetary penalty to the organisation

4. Prosecution for an offence under s55 for deliberate misuse of personal information

In respect of the monetary penalty the following will be taken into consideration when deciding the size of the monetary penalty:-

- The size and sector of the organisation
- The financial resources of the organisation
- The seriousness of the breach
- The number of times the breach has happened

The purpose of the penalty is to promote compliance with the legislation

Glossary

There is a glossary of data protection terms in the guide at Appendix 1

Getting Ready for GDPR

1. **Ensure that all Councillors and Employees know the law is changing** and that the council will need to carry out certain tasks to comply with the legislation. (Think about a briefing or training for council and staff)

2. **Carry Out an Information/Data Audit**

   To do this a Personal Data Audit Questionnaire – See template at

   This questionnaire is designed to help councils (and parish meetings) to audit their personal data. It is important that councillors and staff complete this form as comprehensively as possible. The purpose of a data audit is to find out what data the council is processing, what it is used for, where it is located and who has access to it. It is an important step in assessing whether there are any risks in the type of processing the council carries out. This questionnaire will also provide the basis for an internal register of information that the council processes/stores and this is known as an Information Asset register. The draft Whitehaven Town Council Information Asset Register is shown at Appendix 1

3. **Identify and document the lawful basis for processing and retaining personal data**

   This is important as the Council has to say what the lawful basis for processing data is in its privacy notices. The draft Whitehaven Town Council Privacy Notices are shown at Appendix 1.

   GDPR sets out six lawful bases for processing data. Unless an exemption applies, at least one of these will apply in all cases. It is possible for more than one to apply at the same time. One of the new requirements for Privacy Notices is that the Council must set out in the Privacy Notice which Lawful basis it is relying on. For most councils, the relevant ones will be: 1 – Consent (but not for staff, councillors and other role holders), 2 – compliance with a legal obligation (which includes performance of statutory obligations), 3 – Contractual necessity (for example with contractors), etc. Slightly different lawful bases apply in each of the sample Privacy Notices as some will only apply to staff, councillors and other role holders.

The six lawful bases for processing personal data under the GDPR are:

(a) Consent: the individual has given clear consent for the Council to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract the Council has with the individual, or because they have asked the Council to take specific steps before entering into a contract.

(c) **Legal obligation:** the processing is necessary for the Council to comply with the law (not including contractual obligations).eg electoral register

(d) **Vital interests:** the processing is necessary to protect someone's life.

(e) **Public task/interest:** the processing is necessary for the Council to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.

(f) **Legitimate interests:** the processing is necessary for the Council's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. **This cannot apply to public authorities processing data to perform official tasks.**

4. Policies and Notices including Privacy Notices

Fair processing of personal data involves transparency and providing information – in the form of a privacy notice eg when asking residents of the parish for personal information in a survey etc. These notices need to be more detailed than under the DPA.

Information that must be provided by the council (data controller) must be:

- concise, easily understood and transparent
- written in clear and plan language
- free of charge

It is important to have clear policies and notices, such as the ones listed below:

a) Privacy Notices - see Appendix 1 where there are 3 draft privacy notices, one for residents of the parish and the general public, one for staff, Councillors and role holders in the council and one that is a general privacy notice for use by the council on its website). The notices are based on a template supplied by NALC

b) Data Retention and Disposal Policy – see draft policy and retention document at Appendix 1. This is based on information supplied by CALC and NALC

c) Website Policy – the Council must ensure that it has permission to publish personal data (photos) on it.

d) Staff training policy on GDPR – The Council should ensure that staff and Councillors are aware of the basics of data protection and personal data security.

5. Consent (Article 7)

There are strict requirements about how the Council seeks consent from individuals but since the Council will very often be able to rely on other lawful processing reasons then very often consent will not be required.

There will be some data processing that the Council will want to do as part of normal Council management for which it will not need to obtain specific consent for that particular action eg holding lists of Councillors, managing allotment tenants or contractors suppliers, undertaking payroll and HR function.

It should be noted that Staff and Councillors cannot give valid consent because consent has to be freely given (and it can also be withdrawn at any time). A staff member cannot be said to be freely giving their consent because the balance of power between them and the Council is not equal. A staff member cannot choose to withhold their consent or to exercise their right to withdraw it. If a staff member were to withdraw a right to consent it would put the Council in an impossible situation as it would be obliged to continue to process the personal data whilst the individual carries out their role. A Councillor does not have a free choice to withhold their consent to the processing of their personal data in connection with the role they are performing in the Council. This means that consent is not an appropriate legal basis to process personal data for staff and Councillors.

Consent should be considered as the last resort particularly as it can easily be withdrawn.

One of the most pressing tasks for councils is the need to deal with the issue of consent. The Regulation states that anyone that councils hold information on must give their explicit and informed consent for their data to be retained for a set period of time and processed which means that the person must be made aware of how their information is protected what it will be used for and what the risks are.

The consent element of GDPR is therefore likely to take a lot of staff time.

One of the main changes is that GDPR places a much greater emphasis on record keeping in order to show compliance with the legislation, including documenting consents. It means that the Council cannot just state it is compliant, it has to prove it and produce evidence. To do this there are a number of actions to take such as documenting the decisions the Council takes about processing activities and various other ways that show compliance such as attending training courses.

GDPR states that consent has to be specific, informed, unambiguous and freely given which means that individuals cannot be chased or unduly pressed for their consent

and the Council will need to keep records to evidence that consents have been properly secured.

The Council will also have to consider the position of minors as children under the age of 16 cannot give consent

There are also issues with **"sensitive personal data".** As explained above the Council will need explicit and specific consent from the data subject for the exact purpose or purposes for which any sensitive personal data will be used. (Article 9)

Consent for one type of data processing does not give the Council permission to do anything else with the personal data. The Council may need several different consent forms (or elements within a single form) to cover different areas of data processing within the activities of the Council.

If the Council currently has consent from residents e.g. to send them newsletters or to otherwise keep them informed about council services, facilities or activities, then depending on how it was obtained, it is likely that the Council will need to obtain a new consent because the rules on obtaining consent under the GDPR are very prescriptive making it harder to obtain it. The draft consent form is shown at Appendix 1 and complies with the new requirements of the GDPR. The Council can start using this straight away for residents whose consent it has not yet obtained. For all existing residents and other members of the community that the Council currently regularly makes contact with, The Council should also send out the consent form to "refresh" or renew any existing consents. In addition the Council could remind individuals with whom it has contracts especially sole traders that their name will appear in agendas and minutes with regards to payment. The Council could use this form to obtain their written consent to continue to publish their names in this way. The Consent Form should not be used for staff, councillors and other role holders.

6. Review of Procedures in the Event of a Data Breach

A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Currently, data breaches do not have to be routinely notified to the ICO or others (although the ICO recommends that it is good practice to do so). The GDPR makes informing the ICO and the individuals affected compulsory in certain circumstances e.g. where there is a high risk to the individuals involved, for instance, through identity theft.

The GDPR introduces a new obligation to notify certain breaches to the ICO within 72 hours and in some case data subjects will have to be notified too.

7. **Register/Notify with the Information Commissioner's Office**

Before 25th May 2018, all local councils that process data must be registered with the Information Commissioner's Office via their website. From 26th May 2018, the ICO has confirmed that although there will be no requirement to register/notify under the GDPR, there will be a new annual "data protection fee" which data controllers will be legally required to pay. The amount as yet has not been finalised but will depend on the size of the organisation, its annual turnover and the amount of personal data it processes. Information on this fee will be made available as soon as possible.

8. **Creation of a Data Register**

Controllers and processors must keep and make available to the Information Commissioner's Office, if requested, comprehensive records of data processing. This requires councils to start to keep a log of what data is collected, how and why, where it is stored, who has access to it and whether there is a legal justification to process it. A draft Information Asset Register is attached at Appendix 1.

9. **Subject Access Requests** (Article 15)

GDPR gives individuals more powers to access data that is held about them. It gives individuals the right to know what data the Council holds, why the data is being processed and whether it will be given to a third party. They have the right to be given this information in hard copy (which must be presented in clear, readable terms), and they have the right to have this data deleted. Under these rules, if someone asks for their data (known as a subject access request), the Council must provide the information within one month. A draft Subject Access Policy is attached at Appendix 1.

Resources

Below is a list of further information and useful guidance on GDPR:

- Regulation (EU) 2016/679 of the European Parliament and of the Council
- Data Protection Bill
- NALC Toolkit and Legal Topic Notes available at www.nalc.gov.uk
- The Information Commissioner's Website www.ico.org.uk
- CALC website office@calc.org.uk

APPENDIX 1

1. Glossary: The jargon Explained
2. Information Asset Register
3. Draft Document Retention Policy
4. Draft Whitehaven Town Council and Your Privacy
5. Draft General Privacy Notice
6. Draft Privacy Notice for Staff, Councillors and Role Holders
7. Draft Consent Form
8. Draft Policy for Responding to Subject Access requests
9. Draft Data Protection Impact Assessment
10. Personal Data Audit Questionnaire

Glossary: The jargon explained

Personal data is information about a living individual which is capable of identifying that individual e.g. a name, email address or photo.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data such as collection, recording, organisation, structuring, storage, adaptation etc

Data controller is the person or organisation (Whitehaven Town Council) who determines the how and what of data processing.

Data processor is the person or firm that processes the data on behalf of the controller.

Data subject is the person about whom personal data is processed.

Consent is a positive, active, unambiguous confirmation of a data subject's agreement to have their data processed for a particular purpose. Consent must be easy to withdraw and must be freely given, provided on an opt-in basis rather than opt-out.

Privacy Notice is a notice from a data controller to a data subject describing how personal data will be used and what rights the data subject has.

Processing is anything done with/to personal data (obtaining, recording, adapting or holding/storing) personal data.

Sensitive personal data is also described in the GDPR as 'special categories of data' and is the following types of personal data about a data subject: racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health or condition; sexual life or orientation; genetic data; and biometric data.

Information Asset Register (IAR)

IAR Owner:	Marlene Jewell
Email:	clerk@whitehaventowncouncil.co.uk
Phone:	01946 67366

Introduction

In order to understand your information and how to manage and protect it, it is vital to first understand what we mean by the term 'information asset' and how this definition can simplify the process.

The following definition is provided by the The National Archives:

An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively.

Information assets have recognisable and manageable value, risk, content and lifecycles.

The key concept here is to group your individual pieces of information into manageable portions; if you had to individually assess every individual file, database entry and piece of data you hold you would likely have a list of millions of items and an impossible task. By grouping items together you can make the task achievable.

An information asset is defined at a level of granularity that allows its constituent parts to be managed usefully as a single unit: too broad and you will not have enough detail, too fine and you will have thousands of assets.

Information Asset Register

An 'Information Asset Register' (IAR) is a tool created in order to effectively record the information gathered about the information assets. This allows you to analyse and report on the information assets easily in order to identify the potential risks to your organisation. In this instance we are using an excel spreadsheet but other methods are available.

Developing an Information Asset Register (also called conducting an Information review or information inventory) is a useful tool for information managers. Information Asset Registers can be used for many objectives:

- to plan the implementation of information security across all information assets in an organisation;
- to identify critical systems for disaster recovery and business continuity;
- for risk analysis;
- to inform digital preservation plans and
- to identify information management strategy priorities.

Field Name	Description / Notes
ID #	The unique ID for the asset
Department / Function	Name of the Department responsible for the management of the information asset. Function area of department where the asset resides e.g Department = Human Resources Function = Payroll
Information Asset (IA) Name	The formal name of the Information Asset
Activity / Description	What activity is the asset used for and what are the component record types involved; for example is it a Procedure? Personnel record? Is the asset 'live' or a legacy asset?
Related Process	The related process the activity supports; for example Recruitment Process; Planning Application Process; Business Support
For what reason is the information used?	Details of the why the information is being processed. For example; to ensure that the organisation can manage their accounts
IA Owner Title	The position / job title of the person responsible for the asset
IA Owner Name	Name of the person responsible for the asset
IA Administrator(s)	Details of the Asset administrator and those who create / update the information asset
Asset Type(s)	Electronic (unstructured) Physical (Paper or microfiche for example) System (structured)
Format	The format in which the information is kept; for example: excel / pdf / word doc etc.
Location	Location of the information at rest E.g. Computer Drives, Cloud storage or SharePoint etc. - where hosted? Physical location of hard copies (filing cabinets / archive stores etc.) We appreciate some assets may have been lost due to attack. Please include these.
Master Record	Is this asset considered to be the master record? Is this the original or a is it a copy?
Business Value	Vital - Copeland could not function without this asset Core - Valuable asset, would cause inconvenience if lost
Personal Data	Does the asset contain personal data? YES/NO If so, what? Name, address etc.
Sensitive Personal Data	Does the information contain sensitive personal data? YES/NO If so what? Medical records or Safeguarding information for example.
Access Controls	What access controls are in place? By role, position, permissions or profiles etc. If paper asset what physical access controls are in place?
Security	What security is applied to the Information Asset? Encryption, Password protected etc.
Information Classification	Are information classifications applied to the asset? E.g. Restricted, Sensitive, Private, Public etc.
Is the information shared?	Yes / No
Who is the information shared with?	What third party organisations is the information shared with? Is the information shared with other internal departments?
For what reason is the information shared?	
External Sharing Method	e.g. email, dropbox, published (website or other)
Sharing/ Processing/ Disclosure Protocols or agreements	Is a sharing/processing/disclosure document in place for the transfer of information to a third party organisation? YES/NO
Details of sharing agreement	Title, location and Date of Document
Date Acquired	When was the information acquired?
Date Reviewed	When was the information asset last reveiwed.
Quantity	How many are there? As accurately as possible. If unknown to the nearest 10's/100's/1000's
Retention Period	Does the data have any specific retention requirements?
Risks / Impact	What are the risks and the potential impact in the following circumstances: - loss of confidentiality - loss of availability - loss of integrity Score as below for each L = Low M = Medium H = High e.g. loss of confidentiality could be: Risk = L : Impact = H

ID #	Department / Function	Information Asset (IA) Name	Activity / Description	Related Process
	Whitehaven Town Council	E-mails	Emails sent/received from Councillors Member of Public, outside agencies	
	Whitehaven Town Council	Letters	Letters sent/received from Councillors, Member of Public, outside agencies	
	Whitehaven Town Council	Grant Applications	Applications received from individuals and charitable organisations for grant funding.	
	Whitehaven Town Council	Allotments	Allotments process for administrations of allotment sites including tenancy agreements, annual billing and waiting lists..	
	Whitehaven Town Council	HR Documents	Personnel records including contracts of employment, salary, tax and ni, and pension contributions, training records.	
	Whitehaven Town Council	Invoices	Invoices received/sent from suppliers, contractors or grant applicants.	
	Whitehaven Town Council	General Correspondence	As required.	

For what reason is the information used?	IA Owner Title	IA Owner Name	IA Administrator(s)	Asset Type(s)
Miscellaneous	Clerk	Marlene Jewell	Marlene Jewell Vanessa Gorley	Electronic
Miscellaneous	Clerk	Marlene Jewell	Marlene Jewell Vanessa Gorley	Electronic, physical
Financial	Clerk	Marlene Jewell	Marlene Jewell Vanessa Gorley	Electronic, physical
Allotment administration	Clerk	Marlene Jewell	Marlene Jewell Vanessa Gorley	Electronic, physical
Personnel records	Clerk	Marlene Jewell	Marlene Jewell Vanessa Gorley	Electronic, physical
Financial	Clerk	Marlene Jewell	Marlene Jewell Vanessa Gorley	Physical
Miscellaneous	Clerk	Marlene Jewell	Marlene Jewell Vanessa Gorley	Electronic, physical

Format	Location	Master Record	Business Value	Personal Data
E-mails	Outlook	Yes	Core Business Requirement	Contact details
word doc, pdf	Shared Council drive (Z)	Yes	Core Business Requirement	Contact details
scanned docs, hard copies,	Shared Council drive (Z) and locked filing cabinets	Yes - locked filing cabinets	Core Business Requirement	Contact details, financial details,
word doc, pdf, hard copies	Shared Council Drive (Z) and locked filing cabinet	Yes - locked filing cabinets	Core Business Requirement	Contact details
word doc, pdf, hard copies	Clerks PC, Shared Council Drive (Z) and office safe	Yes - Clerks PC, Shared Council Drive (Z) and office safe	Core Business Requirement	Contact details, NI NO, personal bank details, Salary, Tax, pensions contributions
hard copies	Locked filing cabinets	Yes - locked filing cabinets	Core Business Requirement	Contact details, financial details,
e-mails, hard copies	Outlook and locked filing cabinets	Yes - locked filing cabinets	Core Business Requirement	Contact details, miscellaneous details,

Sensitive Personal Data	Access Controls	Security
Potentially	Permission Based Access	Access controls
Potentially	Password and permission based access	Access controls
No	entrance into office only accessible by passcode on keypad and key in lock, passcode required to access office safe	
Potentially	Password and permission based access - entrance into office only accessible by passcode on keypad and key in lock, passcode required to access office safe	
Yes	Password and permission based access - entrance into office only accessible by passcode on keypad and key in lock, passcode required to access office safe	Password protected
No	entrance into office only accessible by passcode on keypad and key in lock, passcode required to access office safe	
Potentially	Password and permission based access - entrance into office only accessible by passcode on keypad and key in lock, passcode required to access office safe	

Whitehaven Town Council Information Asset Register			
Information Classification	**Is the information shared?**	**Who is the information shared with?**	**For what reason is the information shared?**
Private, restricted, sensitive	Potentially	Requestor, Employees, Councillors, outside agencies,	to respond/inform regarding the request
Not used	Potentially	Requestor, Employees, Councillors, outside agencies,	to respond/inform regarding the request
Confidential	Yes	Councillors	to make a decision on whether or not to award funding to applicants
Not used	No		N/A
Not used	Yes	HMRC and Local Pension provider	to process TAX and NI contributions
Not used	Yes	Employees, Internal Auditor	Payment authorisation and annual audits
Not used	Yes	Requestor, Employees, Councillors, outside agencies,	to respond/inform regarding the request

External Sharing Method	Sharing/ Processing/ Disclosure Protocols or agreements	Details of sharing agreement	Date Acquired
Outlook email	N/A	N/A	N/A
Outlook email	N/A	N/A	N/A
Outlook email/ hard copies	N/A	N/A	N/A
N/A	N/A	N/A	N/A
HMRC Government Gateway website and Pension Providers Sharepoint	N/A	N/A	N/A
Outlook email/ hard copies	N/A	N/A	N/A
Outlook email	N/A	N/A	N/A

Date Reviewed	Quantity	Retention Period	Risks / Impact
N/A	N/A	As appropriate.	Loss of Confidentiality - L/H Loss of Availabilty - L/L Loss of Integrity - L/M
N/A	N/A		Loss of Confidentiality - L/H Loss of Availabilty - L/L Loss of Integrity - L/M
N/A			Loss of Confidentiality - L/H Loss of Availabilty - L/L Loss of Integrity - L/M
N/A	184	As appropriate.	Loss of Confidentiality - L/H Loss of Availabilty - L/L Loss of Integrity - L/M
N/A	N/A	10	Loss of Confidentiality - H/H Loss of Availabilty - H/H Loss of Integrity - H/H
N/A	N/A	100 years	Loss of Confidentiality - L/H Loss of Availabilty - L/L Loss of Integrity - L/M
N/A			Loss of Confidentiality - L/H Loss of Availabilty - L/L Loss of Integrity - L/M

WHITEHAVEN TOWN COUNCIL

RETENTION OF DOCUMENTS POLICY

Adopted by Full Council on _____ Revision Date _____

Retention of Documents Schedule

This retention schedule refers to record series regardless of the media in which they are stored.

Record	Minimum Retention Period	Reason
Financial		
Annual Audited Accounts	Indefinite	Council financial regulations
Annual Return	Indefinite	
Asset register	Indefinite	
Bank paying-in book	Last completed audit year	Audit
Bank Statements including deposit/savings accounts	6 years	Audit, Council financial regulations
Cheque Book Stubs	6 years	Council financial regulations
Grant Applications and record of payment		
Investments	Indefinite	Audit, Management
Paid Invoices	6 years	VAT, Council financial regulations
Paying in receipts	6 years	
Quotations and Tenders (successful)	6 years	Limitation Act 1980 (as amended)
Quotations and Tenders (unsuccessful)	2 years	
Returned cheque records	6 years	
Receipt and payment account(s)	Indefinite	Archive
Receipt book of all kinds	6 years	VAT, HMRC Inspections
VAT returns and records	6 years	HMRC Inspections, VAT, Audit
Insurance		
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
Insurance claims and correspondence	7 years	
Insurance registers	Indefinite	
Insurance schedules	Indefinite	
Insurance valuations	6 years	Unless re-valued
Insurance policies (other than public liability insurance)	While valid	After discontinuation
Public liability insurance policies and premiums paid	21 years	

Staff & Councillors		
Annual leave records	2 years	Operational
Application forms (successful)	Add to Personnel file	Equalities Act
Application forms (unsuccessful applicants)	6 months from appointee duties	Equalities Act
Declarations of Interest	4 years or until they vacate office	
Leavers forms	6 years	
Mayoral expenses/allowance claim forms	6 years	
Members attendance registers	Indefinite	
P45 forms	3 years	
Payroll	12 years	
Personnel Files	6 years after termination of service	Risk of investigation regarding any future litigation
Receipts/Invoices Mayoral	6 years	
Sickness records	3 years	Operational
Staff records	6 years	Operational
Starter forms	6 years	
Superannuation correspondence	Indefinitely	Local Government Pension Scheme
Superannuation records	6 years	Local Government Pension Scheme
Tax & NI details	6 years	Superannuation/HMRC Inspection
Taxable benefit details	6 years	HMRC Inspection
Timesheets	Last completed audit year	Audit and Working time regulations
Council Administration		
Allotment register, plans and tenancy agreements	Indefinite	Audit/Management
Complaints	6 years after resolution of complaint	Operational
Council meeting agendas	Indefinite	Operational
Signed Council and Committee meeting minutes and Minute books	Indefinite	Common practice
Councillors' declaration of office	4 years or until they vacate office	Operational
Draft Minutes	Until the date of confirmation of the minutes	Operational
General correspondence	6 years after correspondence ends	Operational
Information requests	6 years after resolution of request	Operational
Planning Applications	Until there is no longer an administrative requirement	Operational
Policy Documents	Until there is no	Operational

	longer an administrative requirement	
Reports and other documents circulated with agendas	Until there is no longer an administrative requirement.	Operational
Risk Assessments	Once superseded by a new risk assessment or once inactive	Operational
Routine Internal correspondence and papers	Until there is no longer an administrative requirement.	Operational
Title Deeds, Leases, Agreements and Contracts	Indefinite	Audit/Management
Scale of fees and charges	6 years	

Whitehaven Town Council, Room 3, The Civic Hall, Lowther Street, Whitehaven, Cumbria, CA28 7SH

Telephone: 01946 67366 Email: clerk@whitehaventowncouncil.co.uk

---

GENERAL PRIVACY NOTICE

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

Other data controllers the council works with:

- [e.g. other data controllers, such as local authorities
- Community groups
- Charities
- Other not for profit entities
- Contractors
- Credit reference agencies]

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

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

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

- Names, titles, and aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to the services provided by a council, or where you provide them to us, we may process information such as gender, age, marital status, nationality, education/work history, academic/professional qualifications, hobbies, family composition, and dependants;
- Where you pay for activities such as use of a council hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- The personal data we process may include sensitive or other special categories of personal data such as criminal convictions, racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sexual life or orientation.

How we use sensitive personal data

- We may process sensitive personal data including, as appropriate:
  - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
  - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
  - in order to comply with legal requirements and obligations to third parties.
- These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
  - In limited circumstances, with your explicit written consent.
  - Where we need to carry out our legal obligations.
  - Where it is needed in the public interest.
- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

The council will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

We use your personal data for some or all of the following purposes:

- To deliver public services including to understand your needs to provide the services that you request and to understand what we can do for you and inform you of other relevant services;
- To confirm your identity to provide some services;
- To contact you by post, email, telephone or using social media (e.g., Facebook, Twitter, WhatsApp);
- To help us to build up a picture of how we are performing;
- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions;
- To enable us to meet all legal and statutory obligations and powers including any delegated functions;
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury;
- To promote the interests of the council;
- To maintain our own accounts and records;
- To seek your views, opinions or comments;
- To notify you of changes to our facilities, services, events and staff, councillors and other role holders;
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives;
- To process relevant financial transactions including grants and payments for goods and services supplied to the council
- To allow the statistical analysis of data so we can plan the provision of services.

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

What is the legal basis for processing your personal data?

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

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

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 whitehaventowncouncil.co.uk This Notice was last updated in May 2018.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller, Whitehaven Town Council, Room 3, Whitehaven Civic Hall, Lowther Street, Whitehaven, Cumbria CA28 7SH

Email: clerk@whitehaventowncouncil.co.uk

Whitehaven Town Council, Room 3, The Civic Hall, Lowther Street, Whitehaven, Cumbria, CA28 7SH

Telephone: 01946 67366 Email: clerk@whitehaventowncouncil.co.uk

---

PRIVACY NOTICE

For staff*, councillors and Role Holders**

*"Staff" means employees, workers, agency staff and those retained on a temporary or permanent basis

**Includes, volunteers, contractors, agents, and other role holders within the council including former staff*and former councillors. This also includes applicants or candidates for any of these roles.

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, photograph, video, 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 Whitehaven Town Council which is the data controller for your data.

The council works together with:

- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies

We may need to share personal data we hold with them so that they can carry out their responsibilities to the council and our community. The organisations referred to above will sometimes be "joint data controllers". This means we are all responsible to you for how we process your data where for example two or more data controllers are working together for a joint purpose. If there is no joint purpose or collaboration then the data controllers will be independent and will be individually responsible to you.

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.

What data do we process?

- Names, titles, and aliases, photographs.
- Start date / leaving date
- Contact details such as telephone numbers, addresses, and email addresses.
- Where they are relevant to our legal obligations, or where you provide them to us, we may process information such as gender, age, date of birth, marital status, nationality, education/work history, academic/professional qualifications, employment details, hobbies, family composition, and dependants.
- Non-financial identifiers such as passport numbers, driving licence numbers, vehicle registration numbers, taxpayer identification numbers, staff identification numbers, tax reference codes, and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- Financial information such as National Insurance number, pay and pay records, tax code, tax and benefits contributions, expenses claimed.
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to, CCTV footage, recordings of telephone conversations, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries and insurance claims.
- Next of kin and emergency contact information
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process and referral source (e.g. agency, staff referral))
- Location of employment or workplace.
- Other staff data (not covered above) including; level, performance management information, languages and proficiency; licences/certificates, immigration status; employment status; information for disciplinary and grievance proceedings; and personal biographies.
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information and communications systems.

We use your personal data for some or all of the following purposes: -

Please note: We need all the categories of personal data in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing any contractual benefits to you
- Liaising with your pension provider.
- Administering the contract we have entered into with you.
- Management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Conducting grievance or disciplinary proceedings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.
- To undertake activity consistent with our statutory functions and powers including any delegated functions.
- To maintain our own accounts and records;
- To seek your views or comments;

- To process a job application;
- To administer councillors' interests
- To provide a reference.

Our processing may also include the use of CCTV systems for monitoring purposes.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal data.

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.

We may also use your personal data in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest [or for official purposes].

How we use sensitive personal data

- We may process sensitive personal data relating to staff, councillors and role holders including, as appropriate:
  - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
  - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
  - in order to comply with legal requirements and obligations to third parties.
- These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in the following circumstances:
  - In limited circumstances, with your explicit written consent.
  - Where we need to carry out our legal obligations.
  - Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our pension scheme.
  - Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
- 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?

- We do not need your consent if we use your sensitive personal data in accordance with our rights and obligations in the field of employment and social security law.
- 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.
- You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

- We may only use personal data relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.
- Less commonly, we may use personal data relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary 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.

What is the legal basis for processing your personal data?

Some of our processing is necessary for compliance with a legal obligation.

We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract.

We will also process your data in order to assist you in fulfilling your role in the council including administrative support or if processing is necessary for compliance with a legal obligation.

Sharing your personal data

Your personal data will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or where you first give us your prior consent. It is likely that we will need to share your data with:

- Our agents, suppliers and contractors. For example, we may ask a commercial provider to manage our HR/ payroll functions , or to maintain our database software;
- Other persons or organisations operating within local community.
- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS services suppliers
- Payroll services providers
- Recruitment Agencies
- Credit reference agencies
- Professional advisors
- Trade unions or employee representatives

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 responsibilities

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

Your rights in connection with 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.

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, if we start to use your personal data for a purpose not mentioned in this notice.

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on whitehaventowncouncil.co.uk This Notice was last updated in May 2018.

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller, Whitehaven Town Council, Room 3, Whitehaven Civic Hall, Lowther Street, Whitehaven, Cumbria CA28 7SH

Email: clerk@whitehaventowncouncil.co.uk

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.

Whitehaven Town Council, Room 3, The Civic Hall, Lowther Street, Whitehaven, Cumbria, CA28 7SH

Telephone: 01946 67366 **Email: clerk@whitehaventowncouncil.co.uk**

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 _____ _____

_____ _____

_____ _____

_____ _____

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 or from the Town Office at Room 3, The Civic Hall, Lowther Street, Whitehaven, Cumbria CA28 7SH.

You can withdraw or change your consent at any time by contacting the council office.

- We may contact you with regards to your allotment tenancy agreement and the annual rental charge.

- We may contact you to keep you informed about what is going on with the council's allotments including news, events, and meetings. These communications may also sometimes appear on our website, or in printed form.

- We may use your name and photo in our newsletters, bulletins or on our website.

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 post

Please return the form to Whitehaven Town Council, Room 3, The Civic Hall, Lowther Street, Whitehaven, Cumbria CA28 7SH.

If you have any queries as to why you have received this letter then please contact Whitehaven Town Council on 01946 67366.

Yours sincerely

Marlene Jewell

Whitehaven Town Council

Whitehaven Town Council and Your Privacy

Whitehaven Town Council is committed to protecting your privacy when you use our services.

The Privacy Notice below explains how we use information about you and how we protect your privacy.

Why we use your personal information

Do you know what personal information is?

Personal information can be anything that identifies and relates to a living person. This can include information that when put together with other information can then identify a person. For example, this could be your name and contact details.

Did you know that some of your personal information might be 'special'?

Some information is 'special' and needs more protection due to its sensitivity. It's often information you would not want widely known and is very personal to you. This is likely to include anything that can reveal your:

- sexuality and sexual health
- religious or philosophical beliefs
- ethnicity
- physical or mental health
- trade union membership
- political opinion
- genetic/biometric data
- criminal history

Why do we need your personal information?

As a Council we will need to use some information about you to deliver services and support to you and may need to use some information about you to:

- manage those services we provide to you;
- train and manage the employment of our workers who deliver those services;
- help investigate any worries or complaints you have about your services;
- keep track of spending on services;
- check the quality of services; and
- to help with research and planning of new services

How the law allows us to use your personal information

There are a number of legal reasons why we need to collect and use your personal information in delivering public duties.

Each privacy notice explains for each service which legal reason is being used. Generally, we collect and use personal information where:

- it is necessary to perform our statutory duties
- you have entered into a contract with us
- it is necessary to protect someone in an emergency
- it is required by law
- it is necessary for employment purposes
- it is necessary to deliver health or social care services
- you have made your information publicly available
- it is necessary for legal cases
- it is to the benefit of society as a whole
- it is necessary to protect public health
- it is necessary for archiving, research, or statistical purposes
- you, or your legal representative, have given consent

Where we have been required to and you have provided consent to use your personal information, you have the right to remove it at any time. If you want to remove your consent please contact clerk@whitehaventowncouncil.co.uk and tell us which service you're using so we can deal with your request.

We only use what we need!

Where we can, we'll only collect and use personal information if we need it to deliver a service or meet a statutory requirement.

If we don't need personal information we'll either keep you anonymous if we already have it for something else or we won't ask you for it. For example, in a survey we may not need your contact details we'll only collect your survey responses.

If we use your personal information for research and analysis, we'll always keep you anonymous or use a different name unless you've agreed that your personal information can be used for that research.

We don't sell your personal information to anyone else.

What you can do with your information

The law gives you a number of rights to control what personal information is held by us and how it is used by us.

You can ask for access to the information we hold on you

We would normally expect to share what we record about you with you whenever we assess your needs or provide you with services.

However, you also have the right to ask for all the information we have about you and the services you receive from us. When we receive a request from you in writing, we must give you access to everything we've recorded about you.

However, we can't let you see any parts of your record which contain:

- Confidential information about other people; or
- Data a professional think will cause serious harm to your or someone else's physical or mental wellbeing; or
- If we think that giving you the information may stop us from preventing or detecting a crime

This applies to personal information that is in both paper and electronic records. If you ask us, we'll also let others see your record (except if one of the points above applies).

If you can't ask for your records in writing, we'll make sure there are other ways that you can. If you have any queries about access to your information, please contact clerk@whitehaventowncouncil.co.uk or 01946 67366.

You can ask to change information you think is inaccurate

You should let us know if you disagree with something written on your file.

We may not always be able to change or remove that information, but we'll correct factual inaccuracies and may include your comments in the record to show that you disagree with it.

You can ask to delete information (*right to be forgotten*)

In some circumstances you can ask for your personal information to be deleted, for example:

- Where your personal information is no longer needed for the reason why it was collected in the first place
- Where you have removed your consent for us to use your information (where there is no other legal reason us to use it)
- Where there is no legal reason for the use of your information
- Where deleting the information is a legal requirement

Where your personal information has been shared with others, we'll do what we can to make sure those using your personal information comply with your request for erasure.

Please note that we can't delete your information where:

- we're required to have it by law
- it is used for freedom of expression
- it is used for public health purposes
- it is for, scientific or historical research, or statistical purposes where it would make information unusable

- it is necessary for legal claims

You can ask to limit what we use your personal data for

You have the right to ask us to restrict what we use your personal information for where:

- you have identified inaccurate information, and have told us of it
- where we have no legal reason to use that information, but you want us to restrict what we use it for rather than erase the information altogether

When information is restricted it can't be used other than to securely store the data and with your consent to handle legal claims and protect others, or where it's for important public interests of the UK.

Where restriction of use has been granted, we'll inform you before we carry on using your personal information.

You have the right to ask us to stop using your personal information for any council service. However, if this request is approved this may cause delays or prevent us delivering that service.

Where possible we'll seek to comply with your request, but we may need to hold or use information because we are required to by law.

You can ask to have your information moved to another provider (data portability)

You have the right to ask for your personal information to be given back to you or another service provider of your choice in a commonly used format. This is called data portability.

However, this only applies if we're using your personal information with consent (not if we're required to by law) and if decisions were made by a computer and not a human.

It's likely that data portability won't apply to most of the services you receive from the Council.

You can ask to have any computer made decisions explained to you, and details of how we may have 'risk profiled' you.

You have the right to question decisions made about you by a computer, unless it's required for any contract you have entered into, required by law, or you've consented to it.

You also have the right to object if you are being 'profiled'. Profiling is where decisions are made about you based on certain things in your personal information, e.g. your health conditions.

If and when WTC uses your personal information to profile you, in order to deliver the most appropriate service to you, you will be informed.

If you have concerns regarding automated decision making, or profiling, please contact the Data Protection Officer who'll be able to advise you about how we are using your information.

Who do we share your information with?

We use a range of organisations to either store personal information or help deliver our services to you. Where we have these arrangements, there is always an agreement to make sure that the organisation complies with data protection law.

We'll often complete a privacy impact assessment (PIA) before we share personal information to make sure we protect your privacy and comply with the law.

Sometimes we have a legal duty to provide personal information to other organisations. This is often because we need to give that data to courts.

We may also share your personal information when we feel there's a good reason that's more important than protecting your privacy. This doesn't happen often, but we may share your information:

- in order to find and stop crime and fraud; or if there are serious risks to the public, our staff or to
- other professionals;
- to protect a child; or
- to protect adults who are thought to be at risk, for example if they are frail, confused or cannot understand what is happening to them

For all of these reasons the risk must be serious before we can override your right to privacy.

If we're worried about your physical safety or feel we need to take action to protect you from being harmed in other ways, we'll discuss this with you and, if possible, get your permission to tell others about your situation before doing so.

We may still share your information if we believe the risk to others is serious enough to do so.

There may also be rare occasions when the risk to others is so great that we need to share information straight away.

If this is the case, we'll make sure that we record what information we share and our reasons for doing so. We'll let you know what we've done and why if we think it is safe to do so.

How do we protect your information?

We'll do what we can to make sure we hold records about you (on paper and electronically) in a secure way, and we'll only make them available to those who have a right to see them. Examples of our security include:

- Encryption, meaning that information is hidden so that it cannot be read without special knowledge (such as a password). This is done with a secret code or what's called a 'cypher'. The hidden information is said to then be 'encrypted'
- Pseudonymisation, meaning that we'll use a different name, so we can hide parts of your personal information from view. This means that someone outside of the Council could work on your information for us without ever knowing it was yours
- Controlling access to systems and networks allows us to stop people who are not allowed to view your personal information from getting access to it
- Training for our staff allows us to make them aware of how to handle information and how and when to report when something goes wrong
- Regular testing of our technology and ways of working including keeping up to date on the latest security updates.

Where in the world is your information?

The majority of personal information is stored on systems in the UK. But there are some occasions where your information may leave the UK either in order to get to another organisation or if it's stored in a system outside of the EU.

We have additional protections on your information if it leaves the UK ranging from secure ways of transferring data to ensuring we have a robust contract in place with that third party.

We'll take all practical steps to make sure your personal information is not sent to a country that is not seen as 'safe' either by the UK or EU Governments.

If we need to send your information to an 'unsafe' location, we'll always seek advice from the Information Commissioner first.

How long do we keep your personal information?

There's often a legal reason for keeping your personal information for a set period of time, we try to include all of these in our document retention policy.

For each service the schedule lists how long, your information may be kept for. This ranges from months for some records to decades for more sensitive records.

Where can I get advice?

If you have any worries or questions about how your personal information is handled by the Council please contact our Data Protection Officer.

For independent advice about data protection, privacy and data sharing issues, you can contact the Information Commissioner's Office (ICO) at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow

Cheshire SK9 5AF
Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number.

Alternatively, visit ico.org.uk or email casework@ico.org.uk.

POLICY FOR RESPONDING TO SUBJECT ACCESS REQUESTS

1. On receipt of a subject access request it will be forwarded to the Clerk immediately.
2. The Council must correctly **identify** whether a request has been made under the Data Protection legislation.
3. 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. All the personal data that has been requested must be **provided** unless an exemption can be applied.
5. We must **respond** within one calendar month after accepting the request as valid.
6. Subject Access Requests must be undertaken **free of charge** to the requestor unless the legislation permits reasonable fees to be charged.
7. Councillors and managers must ensure that the staff they manage are **aware** of and follow this guidance.
8. 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 Clerk upon receipt of a request.
2. The Council 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. The Council 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, the Council 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. The Council must not withhold personal data because it believes it will be misunderstood; instead, it should provide an explanation with the personal data. The Council 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. The Council may be able to agree with the requester that they will view the personal data on screen or inspect files on our premises. The Council must redact any exempt personal data from the released documents and explain why that personal data is being withheld.

5. This will be made clear on forms and on the council website.

6. The Council will do this through the use of induction, 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, the Council must advise the requestor that they may complain to the Information Commissioners Office ("ICO") if they remain unhappy with the outcome.

9. All letters must include the following information:

   (a) the purposes of the processing;

   (b) the categories of personal data concerned;

   (c) 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 Rules or EU model clauses

   (d) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;

   (e) 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;

   (f) the right to lodge a complaint with the Information Commissioners Office ("ICO");

   (g) if the data has not been collected from the data subject: the source of such data;

   (h) 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

10. Replying to a subject access request providing the requested personal data

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. We are pleased to enclose the personal data yourequested.

Include 1(a) to (h) above.

Copyright in the personal data you have been given belongs to the council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published or otherwisemade available in whole or in part without the prior written consent of the copyrightholder.

Yours sincerely"

11. Release of part of the personal data, when the remainder is covered by an exemption

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. To answer your request we asked the following areas to search their records for personal data relating to you:

- [List the areas]

I am pleased to enclose *[some/most]* of the personal data you requested. *[If any personal data has been removed]* We have removed any obvious duplicate personal data that we noticed as we processed your request, as well as any personal data that is not about you. You will notice that *[if there are gaps in the document]* parts of the document(s) have been blacked out. *[OR if there are fewer documents enclose]* I have not enclosed all of the personal data you requested. This is because *[explain why it is exempt]*.

Include 1(a) to (h) above.

Copyright in the personal data you have been given belongs to the council or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published, or otherwisemade available in whole or in part without the prior written consent of the copyrightholder.

Yours sincerely"

12. Replying to a subject access request explaining why you cannot provide any of the requested personal data

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for*[subject]*.

I regret that we cannot provide the personal data you requested. This is because*[explanation where appropriate]*.

[Examples include where one of the exemptions under the data protection legislation applies. For example the personal data might include personal data is 'legally privileged' because it is contained within legal advice provided to the council or relevant to on-going or preparation for litigation. Other exemptions include where the personal data identifies another living individual or relates to negotiations with the data subject. Your data protection officer will be able to advise if a relevant exemption applies and if the council is going to rely on the exemption to withhold or redact the data disclosed to the individual, then in this section of the letter the council should set out the reason why some of the data has been excluded.]

Yours sincerely"

DPIA ASSESSMENT CHECKLIST

A. Under the GDPR, data protection impact assessments (DPIAs) are mandatory where the processing poses a high risk to the rights and freedoms of individuals. While they can also be carried out in other situations, councils need to be able to evaluate when a DPIA is required.

B. This checklist will help the Council make that assessment and provides a springboard for some of the issues it will need to consider in more detail if it does need to carry out a DPIA.

1. Does the Council need to carry out a DPIA?

(a) What is the objective/intended outcome of the project?

(b) Is it a significant piece of work affecting how services/operations are currently provided?

(c) Who is the audience or who will be affected by the project?

(d) Will the project involve the collection of new personal data about people? e.g. new identifiers or behavioural information relating to individuals

(e) Will the project involve combining anonymised data sources in a way that may give rise to a risk that individuals could be identified?

(f) Will the project involve combining datasets originating from different processing operations or data controllers in a way which would exceed the reasonable expectations of the individuals?

(g) Is data being processed on a large scale?

(h) Will the project compel individuals to provide personal data about themselves?

(i) Will personal data about individuals be disclosed to organisations or people who have not previously had routine access to the personal data?

(j) Will personal data be transferred outside the EEA?

(k) Is personal data about individuals to be used for a purpose it is not currently used for, or in a way it is not currently used?

(l) Will personal data about children under 13 or other vulnerable persons be collected or otherwise processed?

(m) Will new technology be used which might be seen as privacy intrusive? (e.g. tracking, surveillance, observation or monitoring software, capture of image, video or audio or location)

(n) Is monitoring or tracking or profiling of individuals taking place?

(o) Is data being used for automated decision making with legal or similar significant effect?

(p) Is data being used for evaluation or scoring? (e.g. performance at work, economic situation, health, interests or behaviour)

(q) Is sensitive data being collected including:

(i) Race

(ii) Ethnic origin

(iii) Political opinions

(iv) Religious or philosophical beliefs

(v) Trade union membership

(vi) Genetic data

(vii) Biometric data (e.g. facial recognition, finger print data)

(viii) Health data

(ix) Data about sex life or sexual orientation?

(r) Will the processing itself prevent data subjects from exercising a right or using a service or contract?

(s) Is the personal data about individuals of a kind likely to raise privacy concerns or is it personal data people would consider to be particularly private or confidential?

(t) Will the project require contact to be made with individuals in ways they may find intrusive?

2. Other issues to consider when carrying out a DPIA

(a) In addition to considering the above issues in greater detail, when conducting a DPIA, the Council will also need to look at issues including:

(i) The lawful grounds for processing and the capture of consent where appropriate

(ii) The purposes the data will be used for, how this will be communicated to the data subjects and the lawful grounds for processing

(iii) Who the data will be disclosed to

(iv) Where the data will be hosted and its geographical journey (including how data subjects will be kept informed about this)

(v) The internal process for risk assessment

(vi) Who needs to be consulted (DPO, data subjects, the Information Commissioners Office ("ICO"))

(vii) Data minimisation (including whether data can be anonymised)

(viii) How accuracy of data will be maintained

(ix) How long the data will be retained and what the processes are for deletion of data

(x) Data storage measures

(xi) Data security measures including what is appropriate relative to risk and whether measures such as encryption or pseudonymisation can be used to reduce risk

(xii) Opportunities for data subject to exercise their rights

(xiii) What staff or, as appropriate, councillor training is being undertaken to help minimise risk

(xiv) The technical and organisational measures used to reduce risk (including allowing different levels of access to data and red flagging unusual behaviour or incidents)

3. The GDPR requires that councils carry out a DPIA when processing is likely to result in a high risk to the rights and freedoms of data subjects. For a council, examples might include using CCTV to monitor public areas.

4. If two or more of the following apply, it is likely that the Council will be required to carry out a DPIA. This does not apply to existing systems but would apply if the Council introduced a new system.

1. Profiling is in use. Example: The Council monitors website clicks or behaviour and record people's interests. ☐

2. Automated-decision making. Example: when processing leads to the potential exclusion of individuals. ☐

3. CCTV surveillance of public areas. Processing used to observe, monitor or control data subjects. ☐

4. Sensitive personal data as well as personal data relating to criminal convictions or offences. ☐

Large scale data processing. There is no definition of "large scale". However, consider: the number of data subjects concerned, the volume of data and/or the range of different data items being processed. ☐

Linked databases - in other words, data aggregation. Example: two datasets merged together, which could "exceed the reasonable expectations of the user" e.g. you merge your mailing list with another council, club or association. ☐

Data concerning vulnerable data subjects, especially when power imbalances arise, e.g. staff-employer, where consent may be vague, data of children, mentally ill, asylum seekers, elderly, patients. ☐

"New technologies are in use". E.g. use of social media, etc. ☐

Data transfers outside of the EEA. ☐

"Unavoidable and unexpected processing". For example, processing performed on a public area that people passing by cannot avoid. Example: Wi-Fi tracking. ☐

WHITEHAVEN TOWN COUNCIL

Personal Data Audit Questionnaire

Part A:	YOUR INFORMATION	
1	1. Person completing questionnaire a) Name. b) Role. c) Telephone number. d) Email.	 a) Marlene Jewell b) Clerk and Responsible Financial Officer c) 01946 67366 d) clerk@whitehaventowncouncil.co.uk
2	Data controller	Whitehaven Town Council
3	Date you completed this questionnaire	18th May 2018
Part B	**COMMUNICATING PERSONAL DATA**	
4	This section relates to communications with councillors, staff and local residents (including mailing lists) general public. **a) What type of personal data does the council keep?** **b) Where does the council get the personal data from?** **c) Why does the council collect or process the data – what does the council do with the personal data?** **d) Who does the council disclose personal data to?** **e) Do the council or parish meeting minutes contain personal data?** **f) Does the council ever send personal data overseas and if so where to and to which organisation? This might include overseas companies providing database or email services.** **g) Does the council collect any sensitive personal data?** see glossary. **h) If so for what reason?**	 Name, address, email address, bank details, telephone numbers Staff, members of the public, other local authorities, community groups, Councillors For purposes relating to local residents concerns; services and staff, contract management, performance of statutory functions Councillors, staff and contractors carrying out work for the Council, pension providers, HMRC Yes No No N/A

Part C:	**SUPPLIERS, COMPANIES, AND OTHER ORGANISATIONS THE COUNCIL CONTRACTS WITH**	
5	About individuals or representatives of organisations which supply us with services such as for council repairs, or with whom we are in contact	
	a) Who does the council keep personal data about?	Tradesmen, suppliers, advisers, payroll
	b) What type of personal data does the council keep?	Name, contact details, qualifications, financial details
	c) Where does the council get the data from?	Individuals and suppliers
	d) Why does the council collect or process the data?	Payroll and management of staff, Council property maintenance and repairs
Part D:	**GENERAL QUESTIONS ABOUT PERSONAL DATA**	
6	a) How does the council store the personal data collected?	In files in locked filing cabinets and in locked Council safe and electronically.
	b) Does the council take any steps to prevent unauthorised use of or access to personal data or against accidental loss, destruction or damage? If so, what?	All hard copy documents are locked away and anything stored electronically is password protected and passwords are changed regularly.
	c) How does the council manage access to data?	Only the Clerk and Trainee Assistant Clerk have a key and the keypad code to open the exterior door of the office, keys for the locked filing cabinets and they code for the safe. All PC's have individual passwords and the Council operates a clear desk policy.
	d) What is the process involved in giving access to staff or councillors?	Staff have access as stated above and Councillors have access to data by coming into the office to view documents containing personal information on a need to know basis.
7	a) Do any procedures exist for e.g. correcting, deleting, restricting, personal data? If so, please provide details.	No
8	a) Who has access to / is provided with the personal data (internally and externally)?	The Clerk, Trainee Assistant Clerk, Councillors
	b) Is there an authorisation procedure for accessing personal data? If so, please provide details.	No
9	Does the council provide a copy of all existing privacy notices?	No
10	So far as the council is aware, has any personal data which was gathered for one purpose been used for another purpose (e.g. communicating council news?) If so, please provide details.	No

11	Does the council have any policies, processes or procedures to check the accuracy of personal data?	No
12	a) In the event of a data security breach occurring, does the council have in place processes or procedures to be followed? b) What are these?	To report it to DPO/ICO
13	a) If someone asks for a copy of personal data that the council holds about them, i.e. they make a 'subject access request', is there a procedure for handling such a request? b) Is this procedure contained in a written document?	Yes in draft form In draft form
14	Does the council have an internal record of the consents which the council has relied upon for processing activities? e.g. to send council newsletters to residents	No
15	a) Are cookies used on our council website? b) Does the council provide information about the cookies used and why they are used? c) Does the council keep a record of the consents provided by users to the cookies? d) Does the council allow individuals to refuse to give consent?	No No
16	Does the council have website privacy notices and privacy policies?	No
17	a) What data protection training do staff (e.g. council administrator, hall bookings secretary) and councillors receive? b) What does the training involve?	
18	a) Does anyone in the council have responsibility for reviewing personal data for relevance, accuracy and keeping it up to date? b) If so, how regularly are these activities carried out?	All staff Daily
19	a) What does the council do about archiving, retention or deletion of personal data? b) How long is personal data kept before being destroyed or archived? c) Who authorises destruction and archiving?	It is done in accordance with the Council's document retention policy. It is destroyed in accordance with the Council's document retention policy. The Clerk

Part E	MONITORING	
20	a) Please identify any monitoring of the following systems that takes place. 'Monitoring' includes all monitoring of systems including intercepting, blocking, recording or otherwise accessing systems whether on a full-time or occasional basis. The systems are:	
	(i) computer networks and connections	N/A
	(ii) CCTV and access control systems	
	(iii) communications systems (e.g. intercom, public address systems, radios, walkie-talkies)	N/A
	(iv) remote access systems	
	(v) email and instant messaging systems	
	(vi) telephones, voicemail, mobile phone records	
	[Please list anything else].	
	b) Does the council have notices, policies or procedures relevant to this monitoring?	No

ALLOTMENT REPORT

Purpose of the Report

To report back to Members of the discussions held at the Allotment Advisory Group meeting.

1.0 INTRODUCTION

- The Allotment Advisory Group met with the Site Representatives from Crow Park, Cartgate and Sneckyeat on 18/05/2018 to discuss any current issues. The Site Representative from Midgey was unable to attend.

2.0 PRESENT POSITION

2.1 It was reported to the Advisory Group that further to the Advisory Group meeting held on 16.03.2018:

- Full Council had approved the request from Cartgate site to use the plot no 33a as a delivery area.
- That the maintenance contractor had been asked to contact the site reps to arrange a convenient time to carry out site surveys with regards to pest control and also taps.
- Enquiries had been made with the Council's Health and Safety Advisors who had forwarded advice from Sensory Trust with regards to suitable types of surfaces for pathways on the disabled plot at Midgey and that the Council was in the process of obtaining the costings involved.
- The skip provider had said that it would be possible to site a larger 12-yard skip but that they could not be filled with rubble as the wagon wouldn't be able to pick them up as they would be too heavy. It was agreed that the skips would be delivered in September 2018 at the end of the growing season.
- New signs had been installed on the gates of each site.

2.2 It was agreed that:

- The Site Reps would report to the office any plots which they believed were not being cultivated so that office staff could contact the tenant.
- The Council would inform the site reps as to when they were planning on inspecting the sites so that the reps could arrange for somebody to accompany them.
- The maintenance contractor be asked to do the first grass cut at Crow Park.

2.3 The Site Representatives requested:

- That the Council provides some hardcore and get the maintenance contractor to fill the potholes on the access paths at Crow Park.
- That plot 33a at Cartgate have some hardcore put down to enable them to site a permanent container (20ft x 8ft).
- That the Maintenance contractor be asked if it was possible when cutting the grass to cut and clean (remove grass).
- That permanent metal signage be erected with Whitehaven Town Council logo on.
- If there was any way the allocating of plots could be speeded up.
- Permission to remove a privet and erect a fence and gate on Plot 8 Sneckyeat no more than 2 metres high.

3.0 RECOMMENDATION

- Members are asked to note the information at 2.1 and 2.2 and to make a decision with regards to the requests at 2.3.

WHITEHAVEN IN BLOOM REPORT

Purpose of the Report and Recommendation

To report back to Members of the discussions held at the Whitehaven In Bloom Advisory Group meeting

1.0 INTRODUCTION

1.1 A meeting of the Whitehaven In Bloom Advisory Group was held on 11th May 2018.

2.0 PRESENT POSITION

2.1 It was reported that:

- The Ranger has checked on the condition of the existing brackets and had identified that 20 in total were either missing or needed repaired. He had made enquiries as to the cost of these with three companies and had received quotes from two companies.
- The 100 flower baskets that had been ordered were due to be ready for collection during the 1st week of June.
- That 20 large barrels had been purchased and it was agreed that they would be sited at the following areas: 5 in the stobbed area at the Junction of Roper Street/Irish Street (opposite Trinity Gardens); 5 near the Gazebo in the Market Place; 4 underneath the Compass on Strand Street, 2 either side of New Lowther Street, 2 either side of the raised bed adjacent to the traffic lights at Inkerman Terrace/Coach Road and 2 either side of the Welcome to Whitehaven sign at the Pelican Garage.
- The Council had been gifted a replica of The Angel of the North.
- Councillor Maudling had provided a list of businesses he had got verbal permission from to install hanging basket(s)/bracket(s).
- The Yellow Earl had agreed to donate £250.00 for a flower bed adjacent to St Nicholas and that the Chamber of Trade would donate the money to have the raised bed adjacent to the traffic lights at Inkerman Terrace/Coach

Road planted with flowers and that Copeland Borough Council had agreed that they would plant and maintain the bed for £250.00 and this would include watering, weeding, edging and dead edging.

2.2 It was agreed that:

- A letter be compiled to obtain written permission to install hanging basket(s)/bracket(s) and that Councillor Maudling would deliver these face to face to the shops.
- Councillor O'Kane contact Gen 2 and accept the gifted replica of The Angel of the North and that it be sited near Duke Pit Fan House as it is a prominent position and overlooks the town, subject to the agreement of the landowner, thought to be Copeland Borough Council.
- That due to the urgent nature of the job of installing the brackets before the hanging baskets were ready, that a purchase order for 10 brackets be sent to the firm who gave us the best value quote of £350.00 for 20 brackets.
- Enquiries to be made with regards to replanting the 5 large planters in front of the Civic Hall and for the Ranger to carry out the work to reduce the cost.

2.3 Action that has been taken since the meeting:

- Letters have been forwarded to Councillor Maudling to obtain signed permission to install bracket(s)/basket(s).
- 10 Large tubs are due to be collected and sited week ending 25/05/2018 with the remaining 10 tubs being collected and sited week ending 01/06/2018.
- Work has started on removing the grass in preparation for planting on the raised bed adjacent to the traffic lights at the Junction of Coach Road/Inkerman Terrace.
- Topsoil has been purchased to fill the 5 large planters in front of the Civic Hall in preparation for planting paid for out of the Mayors allowance.

3.0 RECOMMENDATION

3.0 That Members approve and note the information and recommendations at 2.1, 2.2 and 2.3.

CALENDAR OF DATES AND TIMES OF COUNCIL MEETINGS, COMMITTEE AND ADVISORY GROUP MEETINGS REPORT

Purpose of the Report and Recommendation

To provide Members with a calendar of dates and times for approval of future meetings of Full Council, Committee and Advisory Groups.

1.0 INTRODUCTION

- Attached at Appendix 1 is a list of scheduled meetings of Full Council, Committee and Advisory Group meetings, with the proviso that it may be necessary to call additional meetings to the ones already scheduled for e.g. Extraordinary Council Meetings.
- All meetings will take place in The Civic Hall unless notified of alternative venues due to availability issues.
- Full Council meetings will take place on the last Thursday of the month and will start at 6:30pm.
- Community Plan meetings will take place on the second Wednesday of the month and will start at 6:30pm.
- Allotment Advisory Group meetings will take place every 2 months but must be on a Friday at 2:00pm to accommodate a Site Reps working hours.
- Whitehaven in Bloom Advisory Group meetings will take place as and when necessary but are likely to take place during office hours.
- Staffing Committee meetings will take place as and when necessary.
- Policy, Resources and Finance Committee meetings will take place every 2 months at 6:30pm.
- Christmas Festivities Advisory Group meetings are to be arranged as and when necessary

2.0 RECOMMENDATION

That Members note the information at 1.0 and approve the list of scheduled meetings at Appendix 1.

Appendix 1

Meeting	Dates
Full Council	28.06.2018
	26.07.2018
	30.08.2018
	27.09.2018
	25.10.2018
	29.11.2018
	31.01.2019
	28.02.2019
	28.03.2019
	25.04.2019
Community Plan Workshops/Training	13.06.2018
	11.07.2018
	08.08.2018
	12.09.2018
	10.10.2018
	14.11.2018
	12.12.2018
	09.01.2019
	13.02.2019
	13.02.2019
Allotments Advisory Group	20.07.2018
	20.09.2018
	16.11.2018
Policy Resources and Finance Committee	04.09.2018
	06.11.2018
	08.01.2019
	05.03.2019