



Summary of initial Data Audit
visit, carried out on 28/02/2020

GDPR DATA AUDIT

Haslemere Town Council

ICO Reg No. ZA557845

Richard Newell
Director
GDPR-info Ltd



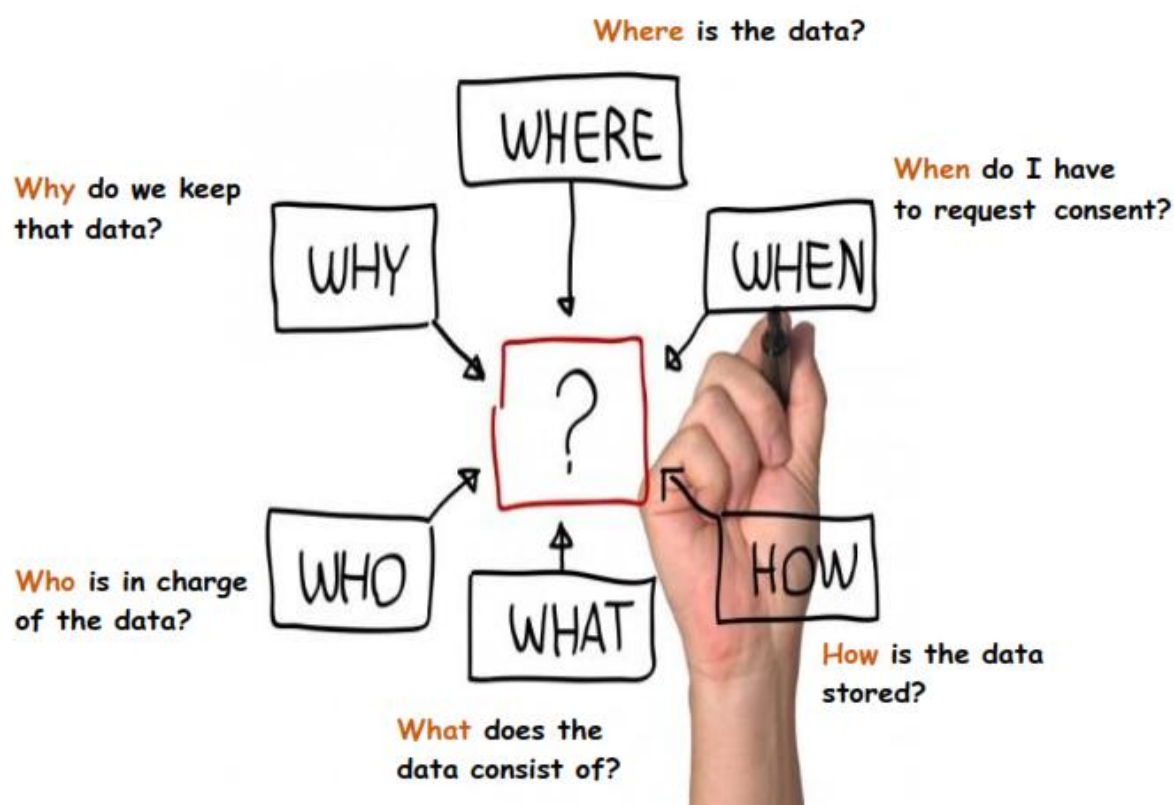
Executive Summary

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

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

It is apparent that Haslemere Town Council does not have many significant issues in the way it handles data now, and once these concerns have been resolved; we feel that they will be working within the guidelines of the new legislation.

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



The diagram above shows how your Council should be viewing the data it holds:



Overview

GDPR Info Ltd have been working with Lisa O'Sullivan, the Clerk of Haslemere Town Council & staff to determine their exposure to the rules of the GDPR. To achieve this, a data audit was carried out and an overview of the results are shown below.

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

It will be necessary for Haslemere Town Council to add to their 'mapping spreadsheet' additional information (CCTV) in order that they can correctly administer & adhere to the GDPR in the future – template will be supplied if not available.



Table of Contents

Executive Summary	1
Overview	2
Findings & Compliancy	5
Questionnaire	5
Councillor Details & Declarations of Interest	10
Employment Records – Staff	11
Employment records / ex-staff & councillors	12
Employment Records – Payroll.....	13
Minutes of Meetings & Confidential Records	14
Correspondence / Emails with local residents	15
Contracts with External Companies.....	16
Electoral Roll.....	17
Local Planning Applications	18
Emergency Plan	19
Data Protection Policies	20
Website	21
Shredding & Data Disposal.....	22
Backups and Computers / Data Sharing / Electronic Items	23
Photocopier	24
Use of Council External Facilities (Rec grounds, Allotments).....	25
Councillor Emails.....	26
Policies.....	27
Training Requirements	28
Administration of GDPR.....	29
Introduction.....	29
Appendix	31
Data Audit Form	32
Data Audit Form	33
Data Audit Form	34
Appendix 2	35
Appendix 3	37
Password Protection / Encryption	38



Understanding the difference	38
Encryption of mobile computing devices.	38
Benefits of encryption.....	39
VPN – Virtual Private Network.....	39
What Is a VPN?	39
What Does a VPN Do?.....	39
Why Is a VPN So Important?.....	40
Do You Really Need a VPN?	40
The Difference Between a Proxy and a VPN	40
VPNs.....	41
Proxy Server	41
Public Wi-Fi Don'ts	41
Public Wi-Fi Do's	42



Findings & Compliancy

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

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

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

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

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

Questionnaire

Area	Question	Yes	No	N/A
Personal Data				
Personal data	Are you processing personal data?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sensitive (special) personal data	Are you processing sensitive personal data?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Children's personal data	Is personal data of children collected and processed?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Scope of application				
EU controller	Are you a controller?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
EU processor	Are you a processor?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Main establishment	Where is the main EU HQ?	UK		
Non-EU controller / processor	Are any group companies located outside the EU that target/monitor EU subjects?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	If so, has an EU representative established in one of the EU States where the data subjects are, been designated in writing (where appropriate)?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Is the EU representative mandated to be addressed (in addition to the controller / processor) by supervisory authorities and data subjects on processing issues?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Joint controllers	Are there any joint data controller relationships?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Lawful grounds for processing				



Lawful grounds for processing	Is there a lawful ground for processing the personal data for each processing operation?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Is there a lawful ground for processing any sensitive personal data for each processing operation?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Consent	How is consent collected?	N/A		
	How is this consent demonstrated?	N/A		
	Can subjects withdraw their consent?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Transparency requirements				
Notification of data subject	Is the data subject notified of processing?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Source of personal data and information provided to data subject	Is data collected direct from the subject and is the required information given to them?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Is the data not collected from the subject and is the required information given to them?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Other data protection principles and accountability				
Purpose limitation	Is personal data only used for the purposes for which it was originally collected?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data minimisation	Is the personal data limited to what is necessary for the purposes for which it is processed?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Accuracy	Are policies and training in place to ensure personal data are checked and where inaccurate are rectified without delay?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Storage limitation (retention)	Do privacy policies incorporate information on retention? Are there procedures in place for archiving and destruction of data?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Integrity and confidentiality	Are appropriate security measures used to protect the data?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Accountability	Can you demonstrate compliance with the data protection principles?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data subject rights				
Access to personal data	Is there a documented policy/procedure for handling subject access requests (SARs)?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are individuals provided with a mechanism to request access to information held about them?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Is the data controller able to respond to SARs within one month?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Data portability	Can data subjects get their personal data in a structured, commonly used and machine readable format?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Erasure and rectification	Are individuals informed of their right to demand erasure or rectification of personal information held about them (where applicable)?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Are there controls and formal procedures in place to allow personal data to be erased or blocked?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Can lists and procedures manage such requests?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Right to object	Are individuals told about their right to object to certain types of processing?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Are there policies to ensure rights can be effected in practice?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Profiling and automated processing	Is profiling based on consent? (if so it this must be explicit).	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Does any profiling use sensitive data?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>



	Does any profiling involve children's data?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data security				
Appropriate technical and organisational security measures	Are the risks inherent in the processing formally evaluated, tested and assessed and have measures to mitigate those risks and ensure the security of the processing been implemented?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Is there a documented security programme that specifies the technical, administrative and physical safeguards for personal data?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Is there a documented process for resolving security related complaints and issues?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Is there a designated individual who is responsible for driving remediation plans for security gaps?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Are industry standard encryption algorithms and technologies employed for transferring, storing, and receiving individuals' sensitive personal information?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Is personal information systematically destroyed, erased, or anonymized when it is no longer legally required to be retained or to fulfil the purpose(s) for which it was collected?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Are steps taken to pseudonymize personal data where possible?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Can the availability and access to personal data be restored in a timely manner in the event of a physical or technical incident?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data breaches				
Breach response obligations	Does the organisation have a documented privacy and security Incident Response Plan and incident identification systems?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are the plan and procedures regularly reviewed and road tested?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are there procedures in place to notify DPAs and data subjects of a data breach (where applicable)?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Is there clear internal guidance explaining when notification is required and what information needs to be reported?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are there clear procedures in place to notify the controller in the prescribed form of any data breach without undue delay after becoming aware of it?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are data breaches documented?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are there cooperation procedures in place between controllers, suppliers and other partners to deal with data breaches?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Have you considered data breach insurance cover? (not mandatory under GDPR)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
International data transfers (outside EEA)				
International data flow mapping	Is personal data transferred outside the EEA?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	What type of personal data is transferred and does this include any sensitive personal data?			
	What is the purpose(s) of the transfer?			
	Who is the transfer to?			



	Are all transfers listed - including answers to the previous questions (e.g. the nature of the data, the purpose of the processing, from which country the data is exported and which country receives the data and who the recipient of the transfer is?)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Is the legal transfer adequacy mechanism for each transfer identified and listed?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Legality of international transfers	Are specific transfers appropriately covered by an implemented adequacy mechanism or covered by an exception?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Transparency	Are data subjects told of any intended transfers of their personal data?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Transfers requested by overseas authorities or courts	Is there a policy for handling requests for disclosure/transfer of personal data to overseas authorities or courts? (The UK has opted out of this provision).	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Other controller obligations				
Technical and organisational measures	What privacy training programmes does the data controller provide for employees?	None at present		
	Are there clear documented policies and procedures for all aspects of GDPR compliance?	SOME	<input type="checkbox"/>	<input type="checkbox"/>
	Do you operate a regular audit review process?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Privacy by design and default	Do policies and procedures build in a requirement to integrate compliance into processing activities?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data Protection Officers (DPOs)	Do you need to appoint a DPO?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	If a DPO is not required, consider whether one should be appointed.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Where a DPO is appointed are escalation and reporting lines in place?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Demonstrating compliance (record keeping)	How many employees does the company have?	3		
	Is sensitive personal data processed?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Are the legal grounds for processing personal data recorded?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data Protection Impact Assessments (DPIAs)	Do you have a process for identifying the need for and conducting (and documenting) DPIAs?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Do you undertake and record prior diligence of service providers?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Are all the stipulated terms included in processor contracts?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Data processor contracts	Are there controller/processor contracts containing all the stipulated terms?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other processor obligations				
Contracts with controllers	Are there controller/processor contracts in place containing the stipulated terms?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Use of sub-processors	Is there written authorisation for existing sub-processing arrangements?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Is there written authorisation for proposed sub-processing?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Has specific or general authorisation been provided?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	If general authorisation, is there a process for informing the controller of any intended changes to processors?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Is the processing subject to a contract including stipulated terms?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>



	Have the same obligations set out in the contract with the controller been imposed on the sub-processor?	<input type="checkbox"/>	<input type="checkbox"/>	✓
Demonstrating compliance (record keeping)	How many employees does the company have?	<input type="checkbox"/>	<input type="checkbox"/>	✓
	Is sensitive personal data processed?	<input type="checkbox"/>	<input type="checkbox"/>	✓
	Are the legal grounds for processing personal data recorded?	<input type="checkbox"/>	<input type="checkbox"/>	✓
Data Protection Officer (DPO)	Do you need to appoint a DPO?	<input type="checkbox"/>	<input type="checkbox"/>	✓
	If a DPO is not required, consider whether one should be appointed.	<input type="checkbox"/>	<input type="checkbox"/>	✓
	Where a DPO is appointed are escalation and reporting lines in place?	<input type="checkbox"/>	<input type="checkbox"/>	✓
Assistance to data controller	Are you able to assist the data controller in ensuring compliance under the GDPR?	<input type="checkbox"/>	<input type="checkbox"/>	✓




Councillor Details & Declarations of Interest

Consisting of:

Full Name:	✓
Full address:	✓
Tel No's: Home or Mobile	✓
Email address:	✓
DoB:	<input type="checkbox"/>
National Insurance #.	<input type="checkbox"/>
Bank Details of individuals	<input type="checkbox"/>
Photo:	✓
Any other Information:	✓
Paper or Digital form	Both

Key Points

-  Signatures Not Redacted on website
-  Computer Files Secure
-  Paper files secure

Who supplied the information?	Subject
Stored Where?	Computer & Backup
Encrypted?	✓
Approx Records	18



Findings & Recommendations

All documents (paper) are currently secured and as they contain personal information including the Councillors signatures.

Electronic records held securely with password & encrypted computer system – however the Declarations of Interests on the Council Website contain actual Signatures (easily used for fraud) – these should be redacted.





Employment Records – Staff

Consisting of:

Full Name:	✓
Full address:	✓
Tel No's: Home or Mobile	✓
Email address:	✓
DoB:	✓
National Insurance #.	✓
Bank Details of individuals	✓
Photo:	<input type="checkbox"/>
Any other Information:	✓
Paper or Digital form	Both

Key Points

-  Computer Data held securely
-  Paper data secure

Who supplied the information?	Subject
Stored Where?	Computer
Encrypted?	✓
Approx Records	3

GDPR COMPLIANCY



Findings & Recommendations

Personnel records held on computer & protected. Single PC used as a 'Server'

Personal Data (paper) held in a locked cupboard/cabinet for protection.




Employment records / ex-staff & councillors

Key Points

Consisting of:


Full Name:	✓
Full address:	✓
Tel No's: Home or Mobile	✓
Email address:	✓
DoB:	<input type="checkbox"/>
National Insurance #.	<input type="checkbox"/>
Bank Details of individuals	<input type="checkbox"/>
Photo:	<input type="checkbox"/>
Any other Information:	✓
Paper or Digital form	Paper

 Personal Data up to date

Who supplied the information? Subject

Who supplied the information?	Subject
Stored Where?	N/A
Encrypted?	<input type="checkbox"/>
Approx. Records	N/A

GDPR COMPLIANCY



Findings & Recommendations

Councillors / Staff: - Up to date

Should any personal information be held, we recommend that only the minimum of data is held for reference – (unless any previous grievance procedures)

Once the term has ended then data should be disposed of as the law believes in data minimisation and not keeping records for longer than is necessary.

Personal Data storage should be held in line with the Councils Data Retention Policy which should be adjusted accordingly as and when. (current policy to be updated)



Employment Records – Payroll

Consisting of:

Full Name: ✓

Full address: ✓

Tel No's: Home or Mobile ✓

Email address: ✓

DoB: ✓

National Insurance #: ✓

Bank Details of individuals ✓

Photo:

Any other Information: ✓

Paper or Digital form Digital

Who supplied the information? Subject

Stored Where? External Supplier

Encrypted? ✓

Approx Records 3

Key Points

- ▲ Data held securely
- ▲ Payroll information received securely

GDPR COMPLIANCY



Findings & Recommendations

Payroll run securely via third party supplier. (processor) – A third party processor agreement should be in place and due diligence carried out to show that the supplier is 'as compliant' as can be for the services they offer.



Minutes of Meetings & Confidential Records

Consisting of:

Full Name:

Full address:

Tel No's: Home or Mobile

Email address:

DoB:

National Insurance #:

Bank Details of individuals

Photo:

Any other Information:

Paper or Digital form Both

Who supplied the information? Internal

Stored Where? Cabinet & Website

Encrypted?

Approx Records N/A

Key Points



Paperwork kept secure

GDPR COMPLIANCY



Findings & Recommendations

Minutes of meetings uploaded to Council website for transparency

Paper copies are held securely

No non-documented / confidential items



Correspondence / Emails with local residents

Consisting of:

- Full Name:
- Full address:
- Tel No's: Home or Mobile
- Email address:
- DoB:
- National Insurance #:
- Bank Details of individuals
- Photo:
- Any other Information:
- Paper or Digital form Both

Key Points



Data held securely

GDPR COMPLIANCY



- Who supplied the information? Subject
- Stored Where? Emails
- Encrypted?
- Approx Records Various

Findings & Recommendations

Digital data (minimal emails etc.) – held on PC until dealt with. We would recommend, when time permits to clear these down in due course and log their removal as per the Councils Data Retention Policy. (to be updated) – data such as residents who assist (with consent) with carol services or the Remembrance Day parades etc.

Data minimisation is key here: - Once the item has been dealt with and you are able to state that the matter has been dealt with, then records should only be kept for a fixed time (unless stated otherwise) – time limits should be set in the Councils Data Retention Policy Document.

Old documents (containing 'personal data' - if not of historical value) should be destroyed in accordance with the Councils Retention Policy



Contracts with External Companies

Key Points

Consisting of:

Full Name:

Full address:

Tel No's: Home or Mobile

Email address:

DoB:


National Insurance #:

Bank Details of individuals

Photo:

Any other Information:

Paper or Digital form Both

 Unknown if Third-Party Data Sharing Agreement in place

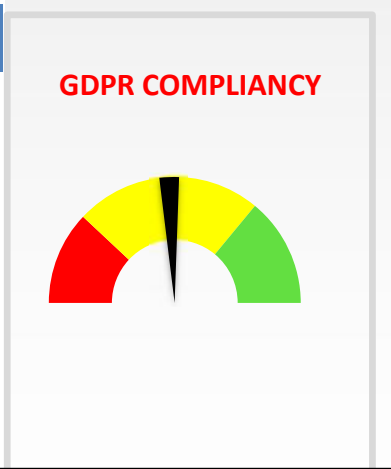
Who supplied the information?

Who supplied the information? Internal

Stored Where? Website??

Encrypted?

Approx Records N/A



Findings & Recommendations

A requirement of the GDPR is that organisations must have agreements in place with those who may have access to data systems (paper / digital)

Website Hosting is through a third-party company– Service Contract in place, however, possibly unsure as to Third-Party Data Sharing Agreement (between Controller & Processor) – this is a requirement of the GDPR. Clerk to ascertain what happens to the data entered via the Contact page on the Council Website as to whether it is stored or just diverted to the Clerks email address. (If stored by host then for how long and when do they delete it?)

Clerk to check also with Payroll & IT company & Photocopier Supplier

Confidentiality Agreement with Cleaners required also



Electoral Roll

Consisting of:

Full Name: ✓

Full address: ✓

Tel No's: Home or Mobile

Email address:

DoB:

National Insurance #.

Bank Details of individuals

Photo:

Any other Information: ✓

Paper or Digital form Digital

Who supplied the information? Internal

Stored Where? Password protected

Encrypted? ✓

Approx Records Numerous

Key Points



Data held securely

GDPR COMPLIANCY



Findings & Recommendations

Electoral Roll is held securely online with password access



Local Planning Applications

Consisting of:

- Full Name:
- Full address:
- Tel No's: Home or Mobile
- Email address:
- DoB:
- National Insurance #:
- Bank Details of individuals
- Photo:
- Any other Information:
- Paper or Digital form Digital

Who supplied the information? Internal

Stored Where? N/A

Encrypted?

Approx Records N/A

Key Points



Data accessed securely

GDPR COMPLIANCY



Findings & Recommendations


Local Planning: Processed by Waverley Borough Council – via online access by the Council Planning Committee.



Emergency Plan

Consisting of:	
Full Name:	✓
Full address:	✓
Tel No's: Home or Mobile	✓
Email address:	✓
DoB:	<input type="checkbox"/>
National Insurance #.	<input type="checkbox"/>
Bank Details of individuals	<input type="checkbox"/>
Photo:	<input type="checkbox"/>
Any other Information:	✓
Paper or Digital form	Both

Key Points

 Emergency Plan data should be held securely when set up

Who supplied the information?	3rd Party
Stored Where?	Paper & Computer
Encrypted?	<input type="checkbox"/>
Approx Records	N/A

GDPR COMPLIANCY



Findings & Recommendations

It was noted that during the conversation with the Clerk that an Emergency Plan is in place.

Personal information gathered should be up-to-date and historical data removed if no longer required. Personal data should be held securely with the data subjects 'consent' and they should be made aware of this and their rights under the GDPR through 'Transparency' to 'Amend' & 'Stop' processing if required. (Privacy Notice)

How long the information is held for should be stated in the Councils Retention Policy and adhered to.

Personal identifiable information (comments from identifiable residents) on the Neighbourhood Plan have been redacted.



Data Protection Policies

Consisting of:

Full Name:

Full address:

Tel No's: Home or Mobile

Email address:

DoB:

National Insurance #:

Bank Details of individuals

Photo:

Any other Information:

Paper or Digital form Both

Key Points



Some Policies are in place and some mandatory ones are missing.



Items require adding to the Data Map

GDPR-Info

Who supplied the information? Unknown

Stored Where? N/A

Encrypted?

Approx Records N/A

GDPR COMPLIANCY



Findings & Recommendations

Few Data Protection Policies are in place; some important documents are missing. GDPR-Info to supply relevant balance of mandatory documents.

Subject Access Request Procedures & Breach Notifications missing & Staff Training Policy

There is a mandatory requirement to MAP (Data Inventory) the Councils data and a spreadsheet can be supplied. It is also known as a Personal Data Inventory or RoPa (Record of Processing Activities) – Clerk has template (this should be kept up to date) (& amended to include CCTV (front door) & New external CCTV)



Website

Consisting of:

Full Name:

Full address:

Tel No's: Home or Mobile

Email address:

DoB:

National Insurance #:


Bank Details of individuals


Photo:


Any other Information:

Paper or Digital form Digital


Key Points

 USA Hosting

 Website Encrypted

 Privacy Notice requires updating

GDPR COMPLIANCY



Who supplied the information? 3rd Party

Stored Where? Website

Encrypted?

Approx Records N/A

Location Information : haslemeretc.org	
Country CodeUS	
Country	United States of America
Name	
Region	California
City	San Francisco

Findings & Recommendations

Website supplied & hosted by Disking Computers Ltd

The website is hosted in the USA – would recommend changing to a UK host as USA privacy laws are not as 'robust' as UK ones.

SSL Encryption is in place – Prevents hacking

Cookie Policy is in place – this has been a legal requirement since 2011 (if used) – however, administering them via a linked site is not acceptable. There should be an easy 'yes' or 'no' for cookies – not a link

Privacy 'Notice' in place – however it does not comply with the 'Transparency' (Article 58 GDPR) of the full right of the data subject & their Right to be informed – this will need to be replaced. (GDPR-Info will supply)

Links to Twitter & Facebook: I would recommend on the page that Haslemere Town Council are not responsible for external information / advertisements which 'may' appear within their links.



Shredding & Data Disposal

Consisting of:

Full Name:

Full address:

Tel No's: Home or Mobile

Email address:

DoB:

National Insurance #:

Bank Details of individuals

Photo:

Any other Information:

Paper or Digital form Paper

Who supplied the information? Internal

Stored Where? N/A

Encrypted?

Approx Records N/A

Key Points



Secure Destruction

GDPR COMPLIANCY



Findings & Recommendations

Shredding of low volume documents is done 'in-house'.

Should there be larger amounts of shredding to do in the future & the Council uses an external company – they must provide a 'destruction certificate'.

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



Backups and Computers / Data Sharing / Electronic Items

Key Points

Consisting of:

Full Name:

Full address:

Tel No's: Home or Mobile

Email address:

DoB:

National Insurance #:

Bank Details of individuals

Photo:

Any other Information:

Paper or Digital form Digital

-  Secure back ups
-  Use of Windows 10 Pro built in Bitlocker secure encryption
-  PC's – password protected

GDPR COMPLIANCY



Who supplied the information? Internal

Stored Where? External Drive

Encrypted?

Approx Records N/A

Findings & Recommendations

Daily Backup of the Admin Officers (used as the office server) to a 'cloud' managed by the Councils IT Supplier. – There must be a third party agreement between the council and the supplier (we will supply)

Password protection is in use for access to the computer

Clerks PC contains HR data: This is not backed up. Recommend that this information be 'hived off' / backed up to a locked directory within the 'Office 365' 'OneDrive' Cloud.

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



Photocopier		Key Points
Consisting of:		<p>GDPR COMPLIANCY</p>
Full Name:	<input type="checkbox"/>	
Full address:	<input type="checkbox"/>	
Tel No's: Home or Mobile	<input type="checkbox"/>	
Email address:	<input type="checkbox"/>	
DoB:	<input type="checkbox"/>	
National Insurance #.	<input type="checkbox"/>	
Bank Details of individuals	<input type="checkbox"/>	
Photo:	<input checked="" type="checkbox"/>	
Any other Information:	<input checked="" type="checkbox"/>	
Paper or Digital form	Digital	
Who supplied the information?		Unknown
Stored Where?		Hard Drive
Encrypted?		<input type="checkbox"/>
Approx Records		N/A

Findings & Recommendations

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

The photocopier also 'auto-orders' replacement toner when low – the Clerk should be aware that as there is an 'external network connection' for the machine to 'reach out' to the Supplier to request toner – there is also the possibility for an external company to have access to the Council network. The Council must be confident that the 'ports' on their network for access by the machine are 'locked down' – so no external inward access is available.



Use of Council External Facilities (Rec grounds, Allotments)

Consisting of:

Full Name: ✓

Full address: ✓

Tel No's: Home or Mobile ✓

Email address: ✓

DoB:

National Insurance #:

Bank Details of individuals ✓

Photo:

Any other Information: ✓

Paper or Digital form Both

Who supplied the information? Subject

Stored Where? Email / File

Encrypted? ✓

Approx Records Various

Key Points

- ▲ Access via Website
- ▲ Payments held & Processed securely

GDPR COMPLIANCY



Findings & Recommendations

Residents are able to book usage of various external sites, the Council Chamber or Allotments or a Recreation ground via the Council Website. Payments are taken via cheque or BACS. Cheques are 'held' by the Admin Officer securely.

I have a concern that the personal information (via the website) can also be viewed/extracted/shared with organisations around the world including the USA. (Companies pay for data which is unknown to the original website owner and the 'host' takes a 'cut') – See Appendix 3



Councillor Emails

Consisting of:

Full Name:

Full address:

Tel No's: Home or Mobile

Email address:

DoB:

National Insurance #:

Bank Details of individuals

Photo:

Any other Information:

Paper or Digital form Digital


Who supplied the information? Internal

Stored Where? PC's

Encrypted?

Approx Records N/A

Key Points

 Emails secure

GDPR COMPLIANCY



Findings & Recommendations

Councillors use the 'haslemeretc.org' which is controlled by the Clerk – a secure way to issue and retract email addresses.



Policies

Policy Area	Already in Place
Data Breach Policy	<input type="checkbox"/>
Staff Privacy Policy	<input type="checkbox"/>
Web Privacy Notice (requires updating)	✓
Retention of Records (requires updating)	✓
Complaints Procedure	<input type="checkbox"/>
Training Policy	<input type="checkbox"/>
Subject Access Request Notice	<input type="checkbox"/>
CCTV	<input type="checkbox"/>
Data Inventory (Data Map) (requires updating)	✓

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

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

The web based Privacy Notice for 'Lion Green' links to a website Cookie Policy – this should be redirected to the correct Privacy Notice – the other links to the Privacy Notices on each of the other 'hiring pages' are correct. The main Privacy Notice requires updating.

The Retention Policy requires updating – Emails, CCTV, FOI requests etc.



Training Requirements

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

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

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



Administration of GDPR

Introduction

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

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

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

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

The areas of GDPR that need to be administered are,

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

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

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



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

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

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



Appendix

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



Data Audit Form	Date of Audit: 28/02/20
Type of Data	Personal non-sensitive/sensitive
Description of data	Various word documents / spreadsheets – paper HR files
Employee responsible	Clerk
Date of consent to hold data	n/a
Where the data is stored	'C' drive on PC
Source of the data	Council business
Purpose of the data	Council business
How the data is protected in its storage	Bitlocker Password Access Paper Files in Locked Cabinet
Usage restrictions	Clerk
Usage rights	Clerk
Usage frequency	Daily
Retention period	Depends on Data
Comments	Recycle Bin 22 items (some contained Personal Identifiable Information) Downloads A number of items (some contained Personal Identifiable Information) It is advisable to remove/delete files from the above areas daily/weekly – can be set up to auto-delete – Clerk to ask IT Supplier



Data Audit Form	Date of Audit: 28/02/20
Type of Data	Personal non-sensitive/sensitive
Description of data	Various word documents / spreadsheets – paper HR files
Employee responsible	Deputy Clerk
Date of consent to hold data	n/a
Where the data is stored	'C' drive on PC
Source of the data	Council business
Purpose of the data	Council business
How the data is protected in its storage	Bitlocker Password Access Paper Files in Locked Cabinet
Usage restrictions	Deputy Clerk
Usage rights	Deputy Clerk
Usage frequency	Daily
Retention period	Depends on Data
Comments	Recycle Bin 452 items (some contained Personal Identifiable Information) Downloads 4567 items (some contained Personal Identifiable Information) It is advisable to remove/delete files from the above areas daily/weekly – can be set up to auto-delete – Clerk to ask IT Supplier



Data Audit Form	Date of Audit: 28/02/20
Type of Data	Personal non-sensitive/sensitive
Description of data	Various word documents / spreadsheets – paper HR files
Employee responsible	Admin Officer
Date of consent to hold data	n/a
Where the data is stored	'C' drive on PC
Source of the data	Council business
Purpose of the data	Council business
How the data is protected in its storage	Bitlocker Password Access Paper Files in Locked Cabinet
Usage restrictions	Admin Officer
Usage rights	Admin Officer
Usage frequency	Daily
Retention period	Depends on Data
Comments	<p>Recycle Bin 247 items (some contained Personal Identifiable Information)</p> <p>Downloads 849 items (some contained Personal Identifiable Information)</p> <p>It is advisable to remove/delete files from the above areas daily/weekly – can be set up to auto-delete – Clerk to ask IT Supplier</p>



Appendix 2

Contact Haslemere Town Council

To find out about the Town Hall staff, their responsibilities and their personal contact details please click [here](#).

If you want more information fill in this form. You will be contacted as soon as possible.
Please fill in all **required fields**.

** Indicates required field*

Your Name *

First Last

Email *

Describe your request *

By submitting this form, you accept our [privacy policy](#).

Phone Number *

Call Us
01428 654305
Office opening hours
Monday, Wednesday, Friday 10am-3pm


Write to Us
Haslemere Town Council
Haslemere Town Hall
High Street
Haslemere
GU27 2HG

Join Us
[Twitter](#)
[Facebook](#)

Social Media Links where it could be shown that HTC are not responsible for external sites.

Hiring Lion Green

Haslemere



Your name *

First Name

Last Name

Organisation Name

Address of applicant *

Street Address

Street Address Line 2

City County

Post Code

Phone Number *

Area Code Phone Number

Lion Green Events

Today | February 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31	1 Feb
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

[+ GoogleCalendar](#)

Application for a permission to use Lion Green, Haslemere

- This application must be completed and returned to Haslemere Town Council and should be submitted a minimum of three months before the required usage date in order to secure the use of Lion Green.
- All events will require Public Liability Insurance to cover the organiser's legal liability to third parties for damage to property or injury to persons that occurs during the course of the event. In addition, the organiser will wish to ensure that all contractors and performers etc. participating in the event have their own public liability insurance to cover their own liabilities. The organiser is also required to take out a general insurance to cover any damage caused to Lion Green.

Link to an external Cookie Notice & Not the correct HTC Privacy Notice



Further processing

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

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on this web page [add URL]. This Notice was last updated in March 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:

Mrs Lisa O’Sullivan, Data Controller, Haslemere Town Council
Email: town.clerk@haslemeretc.org

Current Privacy Notice requires updating to include a statement that your DPO can be contacted via the Clerk. Also missing links

HASLEMERE TOWN COUNCIL DOCUMENT RETENTION SCHEME

1. Introduction

- 1.1 The council recognises the need to retain documentation for audit purposes, staff management, tax liabilities and the eventuality of legal disputes and proceedings.
- 1.2 In agreeing a document retention scheme, the council has addressed these needs, and taken into account its obligations under the Local Government Act 1972, the Audit Commission Act 1998, the Public Records Act 1958, the Data Protection Act 1998, the Employers’ Liability (Compulsory Insurance) Regulations 1998, the Limitation Act 1980, the Employment Rights Act 1996, the Local Authorities Cemeteries Order 1977, the Local Government (Records) Act 1962, the Freedom of Information Act 2000 and the Lord Chancellor’s Code of Practice on the Management of Records Code 2002.

Document Retention Policy on Website states the old Data Protection Act 1998 instead of the GDPR/DPA18



Appendix 3

Insecure first-party requests

haslemeretc.org (<http://haslemeretc.org/>)

Third-party requests

16 requests (16 secure, 0 insecure) to 5 unique hosts.

A third-party request is a request to a domain that's not `haslemeretc.org` or one of its subdomains.

Host	IP	Country	Classification	URLs
ajax.googleapis.com	172.217.19.234	US	Content (Google)	Show (1)
cdn2.editmysite.com	151.101.121.16	FR		Show (8)
fonts.googleapis.com	216.58.209.234	US	Content (Google)	Show (4)
fonts.gstatic.com	216.58.215.35	US	Content (Google)	Show (2)
ssl.google-analytics.com	172.217.18.200	US	Disconnect (Google)	Show (1)

We use Disconnect's [open source list of trackers](#) to classify hosts.

GDPR: [Rec. 69](#), [Rec. 70](#), [Art. 5.1.b-c](#), [Art. 25](#).

Data input to the website can potentially be 'read' by Third Parties in the USA & France

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:

Mrs Lisa O'Sullivan, Data Controller, Haslemere Town Council

Email: town.clerk@haslemeretc.org

General Privacy Policy on current Website – The Clerk is not the Data Controller – the organisation (as a whole) is.



Password Protection / Encryption

Understanding the difference

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

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

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

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

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

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

Encryption of mobile computing devices.

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

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

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



Benefits of encryption

The benefits are

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

VPN – Virtual Private Network

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

What Is a VPN?

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

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

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

What Does a VPN Do?

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

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

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



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

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

Why Is a VPN So Important?

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

Do You Really Need a VPN?

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

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

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

The Difference Between a Proxy and a VPN

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

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

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



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

VPNs

-) A VPN encrypts, or scrambles, data so that a hacker cannot tell what a person is doing online. In other words, a VPN offers a type of tunnel, which is where the data goes. This tunnel cannot be penetrated, and your transmissions cannot be viewed.
-) A VPN is private, and it can make any public network private for those who use them. A VPN can be used on a desktop or any mobile device including laptops, phones, and tablets.
-) A VPN protects data. This data includes instant messages, e-mail communications, downloads, login information, and which sites you visit.
-) A VPN alters your IP address, too. This makes it seem like you are using your computer elsewhere. This makes it possible to access sites like Facebook if they are otherwise blocked.

Proxy Server

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

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

Public Wi-Fi Don'ts

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



-) Take a look at the networks before connecting to them. Make sure you are connecting to the right network and not to a network that is specifically set up to collect information, it might say “free Wi-Fi”.
-) Do not turn on file sharing when connected to public Wi-Fi.
-) If you don't need to connect to a wireless connection, don't leave your Wi-Fi on.
-) Never do any online banking or work with sensitive information when connected to these networks.
-) Do not let anyone see your screen.

Public Wi-Fi Do's

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

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

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