GDPR Audit Report

Haywards Heath Town Council

Richard Newell, Director

GDPR-info Ltd— Blackdown House, The Luth, Wisborough Green, West Sussex. RH14 0BL

T: 01444 245415 **MO:** 07973 315815 **E:** info@gdpr-info.com

Executive Summary

The purpose of this report is to provide Haywards Heath Town Council with feedback from the recent Data Protection Audit; identify areas of weakness and provide a framework, required to meet GDPR requirements over the next few months.

It is apparent that Haywards Heath Town Council does have some significant issues in the way it handles data at the moment. Areas of concern relate to the use and handling of Papers kept, email usage & Accounting data in particular.

It is still not apparent yet whether all previously held marketing data (a noted point) will need to be re-freshed in terms of consent. We are awaiting the report of Working Party 29 to identify what must happen with business data obtained before the implementation of GDPR.(This should be available from the ICO around the 13th April 2018)

There is a requirement to carry out a series of training sessions with the staff & Counsellors of Haywards Heath Town Council. These must be documented and logged against the relevant training files.

Overview

GDPR-*info* have been working with Haywards Heath Town Council to determine their exposure to the new rules in the GDPR. In order to achieve this, a data audit was carried out and an overview of the results is shown below.

It will be necessary for Haywards Heath Town Council to start logging the data they hold in a database in order that they can correctly administer GDPR in the future. In the short term this can be carried out with a simple Excel spreadsheet or using a simple paper-based system that allows them to log the different data sources.

Contents

The following tables outline our findings with scores against specific compliancy with the GDPR.

Findings and Compliancy.

REGISTERED WITH THE ICO (COUNCIL) – **YES**

PERSONAL DATA KEPT OR PROCESSED - BOTH

COUNCILLOR CONTACT DETAILS – N0. COUNCILLORS (**16**)

Consisting of:

Full Name: **YES**

Full address: **YES**

Tel No's: Home or Mobile **YES**

Email address: **YES**

DOB: **YES (Used for Payroll & Pensions)**

Photo: **YES**

Any other Information:

Paper or digital form? **BOTH**

Who supplied the information? **DATA SUBJECT - COUNCILLOR**

STORED WHERE? – **PAPER FILES IN LOCKED CABINET**

Councillor Declaration Of Interest – **ALL SIGNED**

Standard form Used? **YES**

Paper or digital form? **BOTH**

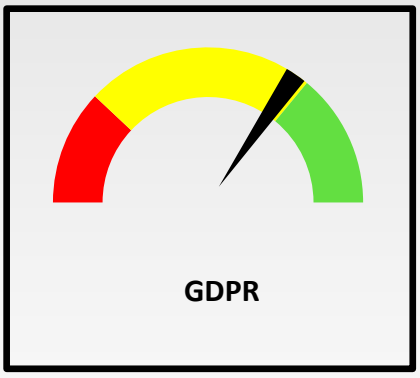
Who supplied the information? **DATA SUBJECT - COUNCILLOR**

STORED WHERE? - **CABINET**

Key Points

- ICO Registration is mandatory
- Data on paper kept in locked cabinet
- Digital copies kept on sever **(*)**
- Server data not encrypted*

GDPR COMPLIANCY



Recommendations

Although Digital data is kept on the HHTC Server – this is not secure and should be encrypted.

Employment Records – Staff

Consisting of:

Full Name: **YES**

Full address: **YES**

Tel No's: Home or Mobile **YES**

Email address: **YES**

DOB: **YES**

NI No. **YES**

Bank Details of individuals (Paper /Digital) **SAGE PAYROLL**

Photo: **NO**

Any other Information: **NO**

Paper or digital form? **BOTH**

Who supplied the information? **STAFF MEMBER**

STORED WHERE? **SERVER & LOCKED CABINET**

Recruitment Records (Previous Councillors Or Staff)

Consisting of:

Full Name: **YES**

Full address: **YES**

Tel No's: Home or Mobile **YES**

Email address: **YES**

DOB: **YES**

Any other Information: **YES**

Paper or digital form? **PAPER**

STORED WHERE? **A4 FOLDER**

Payroll – **SEE SPECIFIC FINDINGS SHEET**

Internal **SAGE**

External – **PENSIONS ONLY**

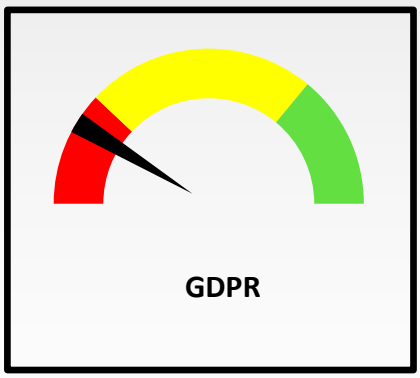
Third Party Company – **WEST SUSSEX COUNTY COUNCIL**

On-line system / manual – **BOTH – backed up to 'C' drive & USB**

Key Points

- Data held securely on electronic payroll system (SAGE)
- Paper docs in locked cabinet
- Non-compliancy with securing data for payroll and accounts.
- Data security backups to a memory stick (unencrypted)

GDPR COMPLIANCY



Recommendations

Whenever data is held on a computer it should be backed up to a suitable media form and not the local drive or a memory stick. A secure partition on an encrypted server should be made available due to the data sensitivity.

Minutes of Meetings

Paper or digital form? – **BOTH (INCLUDING HISTORICAL DOCS)**

STORED WHERE? **LOCKED CABINET**

Non – Documented Records

Paper or digital form? N/A

STORED WHERE? N/A

Correspondence / Emails with Local Residents

Consisting of:

Full Name: **YES**

Full address: **YES**

Tel No's: Home or Mobile **YES**

Email address: **YES**

DOB: **NO**

Any other Information: **YES**

Paper or digital form? **BOTH**

STORED WHERE? **'Z' DRIVE ON SERVER**

Arrangements with Volunteers

Personal Details recorded? **YES**

Consisting of: NAMES

Full Name: YES

Full address: N/A

Tel No's: Home or Mobile YES

Email address: N/A

DOB: N/A

Photo: NO

Any other Information:

Paper or digital form? BOTH

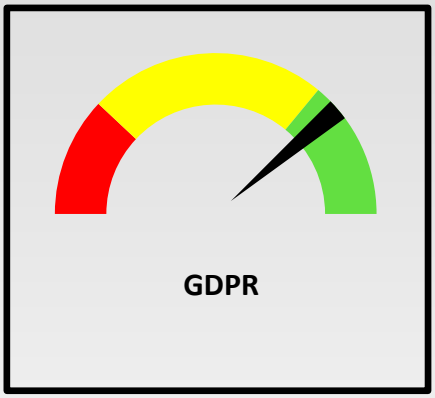
Who supplied the information? DATA SUBJECT

STORED WHERE? SERVER

Key Points

- Minutes stored appropriately
- Data is held on the Server

GDPR COMPLIANCY



Recommendations

Server is not encrypted – this should be done for security reasons

Users of Council Facilities (Halls / Rec Ground / Allotments etc.)

Personal Details recorded? **YES**

Consisting of:

Full Name: **YES**

Full address:

Tel No's: Home or Mobile **YES**

Email address: **YES**

DOB: **NO**

Any other Information: **HIRE CONTRACT ON RBS SYSTEM**

Paper or digital form? **BOTH**

Who supplied the information? **HIRERS**

STORED WHERE? **LOCKED SAFE**

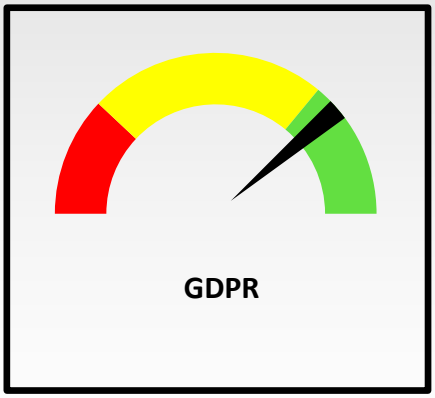
RBS Systems allow for DOB to be collected for:

Allotments for the possibility of offering a discount for pensioners
Also, in their latest release – they are now going to remove / secure next of kin details from the cemetery package to deal with the GDPR.

Key Points

- Data held securely on CRM system
- Paper printouts held securely

GDPR COMPLIANCY



Recommendations

Scanned Paper Records containing data subject's details should be stored securely in a locked cabinet or destroyed once placed on a digital system

CONTRACTS WITH INDIVIDUALS – N/A

ANY AGREEMENTS IN PLACE? N/A

CONTRACTS WITH COMPANIES/CHARITIES

WEBSITE, PCI, GRAVEDIGGERS, STREETLIGHTS, IT SUPPORT, CCTV

BANK DETAILS OF CONTRACTORS / SUPPLIERS - YES

ELECTORAL ROLL – WHERE IS IT (ELECTRONIC OR PAPER)

PAPER STORED IN CABINET

FOI REQUESTS – PAPER OR DIGITAL N/A

COMMUNICATION WITH OTHER LOCAL AUTHORITIES

NOT PERSONAL

COMMUNICATION WITH THIRD PARTIES – N/A

ANY INDIVIDUALS IDENTIFIED IN AN EMERGENCY PLAN

Draft Continuity Plan (Winter Plan) Town Clerk Emails only

LOCAL PLANNING APPLICATIONS

KEPT WITH DISTRICT COUNCIL

ANY HISTORICAL PARISH RECORDS

YES – BOOKS, MINUTES & AGENDAS

ANY BURIAL RECORDS - YES

PLOTS PURCHASED - **YES**

FAMILY NAMES – **YES (Stored in folders under desk)**

GENERAL COMMUNICATIONS BETWEEN STAFF & COUNCILLORS

MINUTES & AGENDAS – YES – INTERNAL EMAILS

NEIGHBOURHOOD PLANS - YES

WORKING GROUP – DATABASE OF INTEREST – **N/A**

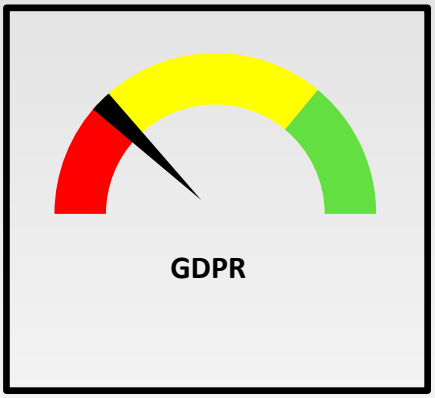
Minimal Personal Data held

ANY BANKING DOCUMENTS WITH PERSONAL DATA - YES

Key Points

- Contracts in Place
- ER stored in cabinet
- Burial Records family names held insecurely
- Bank details stored on non-secure system

GDPR COMPLIANCY



Recommendations

Contracts should be checked with suppliers although there is minimal personal information kept

Bank details should be kept securely

Paper Burial Records should be kept in a locked cabinet for security & not under a desk in a folder

Notices, Surveys, Newsletters

POLICIES – WHAT IS IN PLACE?

Data protection Policy - **YES**

Complaints **NO**

Training Policy **STAFF ONLY**

Fair processing **NO**

SAR Procedure **NO**

Retention of Records Procedure **NO**

Any others? Internal Audit/Email Risk/Equal Opportunities

FOI - **YES**

Website

Security (SSL) **NO**

Design by **'INTOUCH' Audited by Web Design Co 15/03/18**

Data Collection

T & C's - **NO**

Privacy Notice (Separate) **NO**

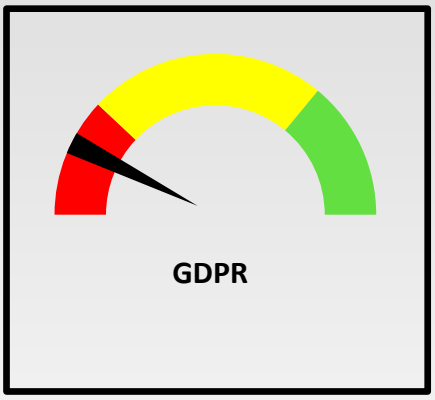
Cookies - **NO**

Data Collection **NO**

Key Points

- Minimal Policies in Place
- Website not secure & no viewable policies

GDPR COMPLIANCY



Recommendations

Urgent requirement to update and employ new GDPR compliant policies also the website requires up to date T' &C's & Privacy Notices & Cookie notice as per 'InTouch Audit'

Having SSL would make it less susceptible to hacking & intruders.

Secure Shredding

Who - **INTERNAL**

How **As and when**

Contract – What's in place & process? **N/A**

Recycle Bin On PC's – **SOME FULL CONTAINING PI**

CCTV – **Is it registered with the ICO - YES**

Retention of Images – **3 DAY CYCLE**

Security of Images (Where) **IN OFFICE ON RECORDER**

Accessed by whom / when & why **????????**

Data Backups

IN-HOUSE/CLOUD/OTHER – **IT COMPANY SET-UP**

WHEN BACKED UP **DAILY**

Security **(As discussed with IT Company)**

Individual PC's are NOT backed up

There is an updated secure firewall on Server

The gateway encompasses Antivirus software

HHTC have no access to this – remotely accessed only

Computers

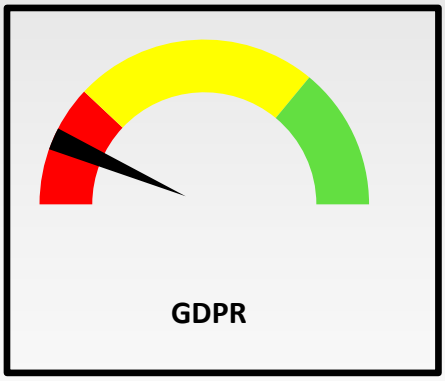
PASSWORD POLICY – **NONE IN PLACE**

INTERNAL HARD DRIVE / EXTERNAL HARD DRIVE / USB – SECURITY – IS IT ENCRYPTED - **NO**

Key Points

- No policy for shredding personal information
- Personal Information held on individual PC's not backed up
- No password policy in place
- Hard Drives not encrypted for best security

GDPR COMPLIANCY



Recommendations

Policy required for shredding personal data documents & a log of it is required.

Staff Training in regularly emptying Trash on Desktop as a standard daily task

Server requires encryption on it to be secure as do PC's and Laptops

All information should be held on the Server in the respective 'drive' & not on the local drive of a desktop computer

Introduce a change password policy for the PC's & Staff training in this.

Children

Any information? N/A

Email Communications:
Retention periods - **NONE**
Security – **DOCUMENTS VIA DROPBOX**
Email Addresses – **Use of HHTC .gov addresses**
Attached Documents

Photocopiers**: YES – Hard drives not cleared down**

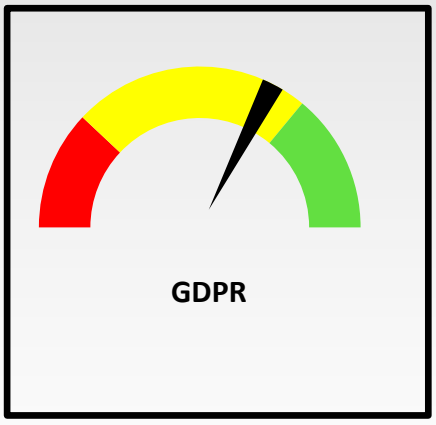
BYOD: (Bring Your Own Device)

Accessing Emails via Councillor Electronic Devices - YES

Key Points

- Secure Dropbox Account
- Use of Secure .gov emails
- Photocopier Hard drive needs checking

GDPR COMPLIANCY



Recommendations

Retention Policy needs to be implemented for emails as kept for a long time

Make sure that '.gov' email addresses are NOT being forwarded to normal 'personal' emails such as 'Gmail & Yahoo' as these can be easily hacked. (To be discussed in a Councillor Training session)

Make Councillors aware of the security risks of accessing Council emails & documents on their own electronic devices (BYOD)

Main issues from the Initial Report

The purpose of this section is to provide Haywards Heath Town Council with a description of the work they need to commence in order to make themselves GDPR compliant.

Whilst we felt that most data issues were relativley problem free, there were major areas of concern in respect of data security & computer encryption and the lack of consent / permission obtained from data subjects to hold their data either in Microsoft outlook or Microsoft Excel files.

Data Security. There was a lack of awareness of how important it was to keep 'personal information' secure.This was found evident where Lever arch files containing some sensitive information were kept 'under a desk' – items such as these should be kept securely in a locked cabinet when not in use.

Absolutely critical to Haywards Heath Town Council implementation of GDPR compliancy is the awareness of keeping electronic data secure, whether it be either for the 'public' or the staff. It is not acceptable to backup a database to a USB stick. Firstly our findings showed (after discussing their IT Systems with the IT company looking after the PC's and related Server) that the PC's don't get backed up to the main server and furthermore the USB stick is not encrypted (as used in the accounts area) – so it could get damaged, lost or stolen and that would certainly cause a data breach – which would require you to inform your Data Protection Officer immediately due to staff personal information being possibly breached.

Greater concern was noted in the use of Microsoft Outlook as an bulk email server. It was not meant for this purpose and the use and inflexibility of it could lead to many issues of breaches. There is no place to 'flag' consent & unsubscribes. We would whole heartedly recommend the use of some dedicated software such as Mailchimp – where you can manage emails correctly in a non complicated manner.

We also found that the main server's hard drives are not encrypted and we would therefore recommend that this be changed – to be discussed with the IT provider.

HHTC Website is not supported by SSL Encryption – so could be easily hacked. We would recommend that HHTC purchase an SSL Licence for its protection.

We would also recommend a rotating password change monthly for all PC users. (To be discussed with IT provider).

Similarly Haywards Heath Town Council must commit to some system of administration of all the tasks they wish to undertake in relation to GDPR. All the work they carry out from now on must be documented and stored, preferably in a spreadhsheet showing where data is kept, how it is stored, why you keep it, when do you need to ask for consent to keep it, what does the data consist of and who is in charge of the data. (Digital & Paper).

Documents & Policies

Work must start now on ensuring that Haywards Heath Town Council has documented and stored the relevant policy documents relating to GDPR and data protection. We will provide the relevant ones as required bespoke to your requirements.

- A Data Breach Policy
- An internal Council Privacy Policy
- A Staff Privacy Policy for the staff handbook
- A Web Privacy Notice
- A Subject Access Request Notice
- Retention of Records list (some to be discussed internally)
- Training Policy

Data Breach Requirements

Introduction

Data breaches are very rarely from the outside of a company and will normally occur because an employee has been negligent or even possibly dishonest.

Areas for data breach include:

- Loss of equipment
- Insecure Passwords
- Opening 'phishing emails'
- Random websites (dropping malicious code)
- External hacking through firewalls

Key Points

- SECURITY
  Ensure all laptops, USB sticks and mobile devices holding data are encrypted.
- EMAILS
  Ensure all staff understand the importance of not clicking on links in emails
- TELEPHONE
  Are your staff sure who they are talking to?

Action in the event of a breach

- Contact your Data Protection Officer immediately
- Identify size and type of data breach
- Ensure breach is sealed
- Report breach within 72 hours

Training Requirements

Introduction

It will be necessary for Haywards Heath Town Council to introduce a section on Data Protection in all their staff & Member induction training courses.

GDPR-info will be delivering key person training to the Staff & Counsellors which will cover items in this report and the risks involved to understand how damaging this could be for the Council.

Training Subjects

- Administration;
- Council Policy about the GDPR;
- Use of data,
- Controlling and Reporting Data Breaches,
- Data Subjects' individual rights;
- Managing Consent

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 Haywards Heath 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 (see Data Breach), it makes sense to have this information readily available rather than having to assemble it from scratch at the time.

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

The areas of GDPR that need to be administered are,

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

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

- Subject Access Requests – Keep a Record of
    - Right to Object

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

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

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

Website Issues

We identified some areas where we believe that Haywards Heath Town Council does not meet GDPR requirements.

Privacy Notice.

This will need to be written.

GDPR requirements for a privacy policy are:

- Identity and contact details of the controller and where applicable, the controller's representative) and the data protection officer
- Purpose of the processing and the legal basis for the processing
- The legitimate interests of the controller or third party, where applicable
- Categories of personal data
- Any recipient or categories of recipients of the personal data
- Details of transfers to third country and safeguards
- Retention period or criteria used to determine the retention period
- The existence of each of data subject's rights
- The right to withdraw consent at any time, where relevant
- The right to lodge a complaint with a supervisory authority
- The source the personal data originates from and whether it came from publicly accessible sources
- Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data
- The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences

Cookie Control.

There does not appear to be a cookie warning banner appearing on the Haywards Heath Town Council website.

This has been a requirement for several years.

Data Retention and Disposal Policy – A core principle of the GDPR is that data should not be retained for longer than is reasonably necessary to enable the processing for which that data was obtained to take place ("storage limitation"). Haywards Heath Town Council will therefore need to be able to demonstrate that data is retained for an appropriate period. A key way to demonstrate that thought has been given to this matter is to develop a policy that provides guidelines in relation to appropriate retention periods for certain documents. This will likely include details about the measures Haywards Heath Town Council is taking to ensure the security of that data both during the period whilst it is retained and in relation to the way it is "disposed".

Subject Access Requests ("SAR") policy – Certain rules relating to SARs change under the GDPR. The changes should be documented in a revised policy so that those involved in handling such requests are aware of the new rules, including revised time periods for responding to SARs, the increased information that must be provided to employees making a SAR, the extent of the search. Beyond ensuring that the new SAR procedure complies with the text of the GDPR, any new procedure is likely to include at least one meeting with the person making the SAR to clarify the scope of the SAR and discuss relevant arrangements for responding. The policy is also likely to reserve the employer's right (in appropriate circumstances only) to extend the deadline for responding to a SAR and potentially charging a fee (or not responding to a SAR at all).

Personal Data Breach Notification and Response plan – The GDPR will mean new mandatory data breach reporting obligations as set out in our recent article. Haywards Heath Town Council will need an appropriate procedure in place to ensure that personal data breaches are handled consistently and correctly across the organisation and that (amongst other things) staff know what to do should they become aware of such a breach.

Legitimate Interests policy – As outlined above, one of the potentially lawful grounds for processing personal data arises where the processing is necessary for the purposes of the legitimate interests of the employer. When relying on this ground, Haywards Heath Town Council need to have a clear and documented process in place for assessing whether in any circumstance; it can validly rely on this ground. Accordingly, a policy which sets out some typical legitimate interests of the employer is highly recommended. This will also detail the process that the employer will follow to ensure in relation to any new processing activities, that (on balance) any such legitimate interests do not override by the rights and freedoms of the employee. The documentation aspect of this is essential to comply with the new GDPR principle of accountability i.e. being able to prove compliance if called upon by the ICO.

Data Security

After discussing the various PC's and Server with the IT company looking after Haywards Heath Town Council, we feel that they need to consider the following areas and ensure that their data security meets these minimum requirements.

Encryption and Password Protection: The differences

There is a considerable amount of misunderstanding out in the business world regarding the protection of personal data and information. For a very long time, people have used passwords to prevent access to things – most notably, Windows or Mac desktops themselves. But password protection is very different from encryption.

Passwords

When data is password protected, it's as if you've gathered all of your data, in its original, readable form, put it into a lock box, and locked the box with a password or passcode. The box is protected by the passcode, but if the lock box is not particularly strong and someone is able to break into it, then getting at all your valuable data is simple.

The most obvious, and perhaps most dangerous, example of simple, password protected data is right in front of you: your Windows or Mac desktop or laptop. Even a novice hacker knows there are several very easy ways to get around the OS passwords and get directly at your data: First, there are CD-based tools readily available on the Internet that someone can use to boot your PC, read your supposedly super-secret password, and then have unfettered access to everything – including Outlook email. Second, there's the brute force method: someone can simply pull the hard drive out of your PC, hook it up to another PC via an external hard drive enclosure, and voila, have access to everything on the hard drive.

Encryption

When you encrypt data, it's as if you take your data, first put it through a shredder with all the shredded pieces falling into the lock box, and then protect the box with a passcode. If someone were to break into the lock box, all they would find are shredded bits of paper, very effectively indecipherable. They key is the passcode. If you enter the passcode, then the shredded bits of paper in the lockbox magically go the reverse direction through the shredder; all the pieces are put back in their original format.

Encryption is built into Mac operating systems and most high end copies of Windows 10 support BitLocker. Alternatively there are software solutions available – but obviously you must ensure that they are safe. (TrueCrypt is no longer a safe alternative for earlier Windows operating systems)

Potential Problems with encryption

Encryption's greatest strength can also be its greatest detraction: if you've used a strong encryption algorithm and you forget your passcode, then the data in that lock box are gone forever; there is no

“back door” or special key to retrieve the data. They're gone. If you haven’t backed up that data, in unencrypted format, then they are simply irretrievable.

Encryption recommendations

We recommend that Haywards Heath Town Council encrypt all of the following hardware:

- Laptops that go outside the building or hold any personal data including email addresses:
- PCs that have personal data stored on local drives.
- All USB sticks – these should NOT be used now.
- Mobile devices such as phones and iPads which have Council related data that includes personal data.

Obviously personal data on a personal phone not relating to the company is exempt from any requirement.

1: Practice the principle of least privilege and put policies in writing

The "least privilege" policy, operates on the assumption that all data is off-limits to a given user unless that user is explicitly given access to it. Unless a user has a demonstrated need to have access to a particular file, he/she can't access it.

Policies should be specific and give examples of what's prohibited. Haywards Heath Town Council employees may not understand, unless you spell it out, that emailing a company document as an attachment to someone outside the network (or even to their own home account) is just as much a violation of policy as copying that document to a USB drive and physically taking it out the door.

2: Set restrictive permissions and audit access

The first step in protecting data is to set the appropriate permissions on data files and folders.

You should give users the lowest level of permissions possible for them to get their work done. For example, give Read Only permissions to prevent users from modifying files. You can also set up auditing on files and folders that contain

3: Use encryption

4: Implement rights management

5: Restrict use of removable media

One of the most popular ways to sneak digital information out of an organisation is by copying it on some sort of removable media or device. Haywards Heath Town Council could permanently restrict the installation of USB devices by removing the ports physically or filling them with a substance, however this may seem excessive and with the growing flexibility of USB port not advisable.

6: Keep laptops under control

7: Set up outbound content rules

Firewalls can keep specified traffic from leaving your network.

You can also set up your mail server to block sending of outbound attachments.

8: Control wireless communications

Keep track of wireless networks that may be available from your company premises and, if possible, block their signals. Do not publish wireless access passwords on meeting room notice boards for instance

9: Control remote access

Your users don't have to be on site to take corporate data away with them. With the popularity of telecommuting and working on the road rising all the time, users can access the company network via various remote access technologies.

10: Beware of creative data theft methods

Remember that your data can walk out in many different formats. A user can print out a document and carry it out in paper form or a thief can steal printed documents from trash cans if the documents haven't been shredded. Even if you've implemented a technology such as rights management to prevent copying or printing documents, someone could take a digital or film photograph of the content onscreen or even sit and copy the information by hand. Be aware of all the ways your data can leave the premises and take steps to protect against them.

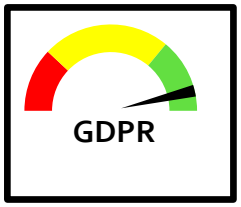
APPENDIX

The following data was compiled from Auditing each area (department) of the Council and determining from each member of staff what data was held and for what purpose it was used to provide an understanding of the procedures currently in place.

Our findings are as follows:

Date of Audit:	19/03/2018
Status of Data	Live
Type of Data	Paper Files
Description of data	Deeds & Registry of Grants
Employee responsible	HHTC
Date of consent to hold data	None
Where the data is stored?	Locked Safe
Source of the data	Relatives of deceased
Purpose of the data	Legal Documents
How the data is protected in its storage?	Secure Storage
Usage restrictions	n/a
Usage rights	n/a
Usage frequency	n/a
Is the data shared?	No
Who is the data shared with?	n/a
Retention period	Indefinitely
Comments	Names & addresses of Next of kin of the deceased

Findings: - Minimal data held and securely stored - **COMPLIANT**



Date of Audit:	19/03/2018
Status of Data	Live
Type of Data	Spreadsheet
Description of data	Allotment Databases (2) Name & address & Invoice number
Employee responsible	HHTC
Date of consent to hold data	Date of Application
Where the data is stored?	Server
Source of the data	Applicant
Purpose of the data	Contact for Invoices
How the data is protected in its storage?	Server backup
Usage restrictions	No permissions
Usage rights	Contractual Agreement
Usage frequency	
Is the data shared?	No
Who is the data shared with?	n/a
Retention period	12 months
Comments	Handwritten waiting list – asked for consent – Written in book on desk

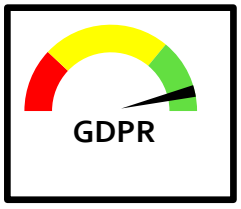
: -

Findings Minimal data held however paper data not securely stored

Recommendations: - Allotment Waiting list should be made secure

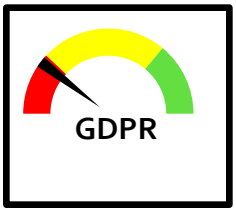
Date of Audit:	19/03/2018
Status of Data	Live
Type of Data	Spreadsheet
Description of data	Town Twinning Data
Employee responsible	Maria (HHTC)
Date of consent to hold data	Unknown
Where the data is stored?	Server
Source of the data	HHTC
Purpose of the data	Details of Town Twinning Events
How the data is protected in its storage?	Server Backup
Usage restrictions	unknown
Usage rights	n/a
Usage frequency	Ad-hoc
Is the data shared?	No
Who is the data shared with?	n/a
Retention period	Non personal after event
Comments	

Findings: - Minimal data held and securely stored - **COMPLIANT**



Date of Audit:	19/03/2018
Status of Data	Live
Type of Data	Spreadsheet
Description of data	Sponsorship list for Town Twinning Gala
Employee responsible	Maria (HHTC)
Date of consent to hold data	None
Where the data is stored?	Server
Source of the data	From Internet
Purpose of the data	Find list sponsors
How the data is protected in its storage?	Server Backup
Usage restrictions	unknown
Usage rights	unknown
Usage frequency	Ad-hoc
Is the data shared?	no
Who is the data shared with?	n/a
Retention period	Unknown
Comments	Consent required for Individuals & informed About linking names to companies

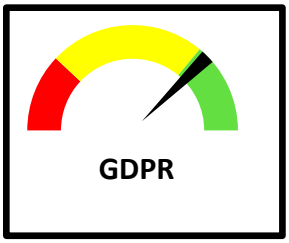
Findings: - Securely stored – however consent is required from individuals as it was found that the data obtained was from 'scraping' the internet – this not acceptable.



We would recommend that data be purchased from a reputable source when consent has been double opted-in and any contacts should be through non-personalised email addresses or telephone if you feel there is a legitimate interest to contact a company for finding sponsorship (making sure first that they are not on the 'CTPS' – Corporate Telephone Preference Service)

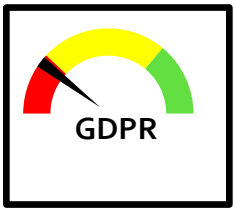
Date of Audit:	**19/03/2018**
Status of Data	Live
Type of Data	RBS Data (Bookings)
Description of data	Bookings for Hall
Employee responsible	Brenda (HHTC)
Date of consent to hold data	n/a
Where the data is stored?	Server
Source of the data	Applicant (Public)
Purpose of the data	Booking Hall Space
How the data is protected in its storage?	Server
Usage restrictions	Limited to 3 PC's
Usage rights	Limited to 3 PC's
Usage frequency	Daily
Is the data shared?	Unknown
Who is the data shared with?	
Retention period	Unknown
Comments	Name/Email (x2) Address/co. name/ Tel no. (x3) Different Username & Password for login

Findings – A secure system which is **COMPLIANT**



Date of Audit:	19/03/2018
Status of Data	Live
Type of Data	Paper
Description of data	Concessionary Rail code paperwork
Employee responsible	Front Desk
Date of consent to hold data	Implied on application
Where the data is stored?	Paper format
Source of the data	Applicant
Purpose of the data	Apply for Rail discount
How the data is protected in its storage?	Not
Usage restrictions	n/a
Usage rights	n/a
Usage frequency	Ad hoc
Is the data shared?	No
Who is the data shared with?	n/a
Retention period	All records kept
Comments	

Findings – Minimal data held – However it is on the front desk and this is not a secure area and there is no set retention period for this data

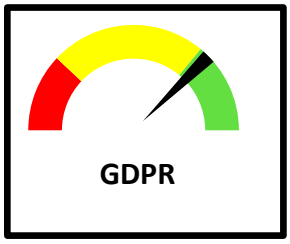


Date of Audit:	19/03/2018
Status of Data	Processing
Type of Data	Paper
Description of data	County Council Enquiry Trace form
Employee responsible	Helen (HHTC)
Date of consent to hold data	Unknown
Where the data is stored?	Paper file (unlocked Cabinet)
Source of the data	County Council
Purpose of the data	Work for Highways Dept
How the data is protected in its storage?	Cabinet
Usage restrictions	n/a
Usage rights	n/a
Usage frequency	Ad hoc
Is the data shared?	No
Who is the data shared with?	n/a
Retention period	Unknown
Comments	

Findings – Minimal data held - **COMPLIANT**

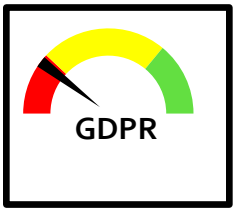
We would recommend setting up a set retention period for this

Data – say for 12 months and then the previous year could be cleared down



Date of Audit:	19/03/2018
Status of Data	Live
Type of Data	Paper
Description of data	Funeral Director – Name of Next of kin with address
Employee responsible	Helen (HHTC)
Date of consent to hold data	n/a
Where the data is stored?	Paper file
Source of the data	Funeral Director
Purpose of the data	To log deaths
How the data is protected in its storage?	File under desk
Usage restrictions	n/a
Usage rights	n/a
Usage frequency	Ad hoc
Is the data shared?	No
Who is the data shared with?	n/a
Retention period	No retention period
Comments	

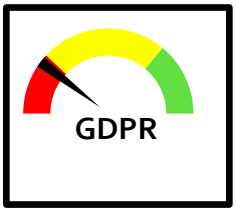
Findings – Sensitive data held and not securely stored



We would recommend that this information should be securely stored in a locked cabinet when not being used and not stored in a folder under the desk

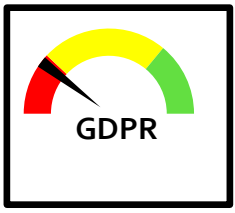
Date of Audit:	**19/03/2018**
Status of Data	Live - Processing
Type of Data	Paper
Description of data	Memorials Data (Same as funeral deeds)
Employee responsible	Helen (HHTC)
Date of consent to hold data	Ongoing
Where the data is stored?	Folder/File
Source of the data	Funeral Director
Purpose of the data	Memorial Headstones
How the data is protected in its storage?	Not
Usage restrictions	n/a
Usage rights	n/a
Usage frequency	n/a
Is the data shared?	No
Who is the data shared with?	n/a
Retention period	On going
Comments	

Findings – Sensitive data held and not securely stored



We would recommend that this information should be securely stored in a locked cabinet when not in use.

Date of Audit:	19/03/2018
Status of Data	Live
Type of Data	Outlook Group
Description of data	Charity invitation Databases (2)
Employee responsible	Fatima (HHTC)
Date of consent to hold data	None
Where the data is stored?	Server
Source of the data	Gathered from Charities (Historical)
Purpose of the data	Ongoing relationships with companies
How the data is protected in its storage?	Server Backup
Usage restrictions	No consent flag
Usage rights	No consent flag
Usage frequency	Bi-annually
Is the data shared?	No
Who is the data shared with?	n/a
Retention period	Ongoing
Comments	Nothing showing in Outlook that Consent has been given

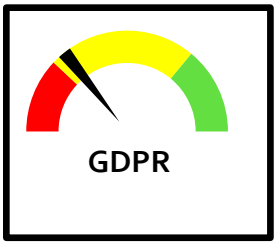


Findings – No visual consent obtained from the data subjects

We would recommend adding a 'consent' flag in the outlook vCard Notes box to categorise consent.

Date of Audit:	19/03/2018
Status of Data	Live
Type of Data	Outlook Contacts
Description of data	Dementia Call Group
Employee responsible	Fatima (HHTC)
Date of consent to hold data	None given
Where the data is stored?	Server
Source of the data	Steering Group Volunteers
Purpose of the data	Steering Group for Dementia Sufferers
How the data is protected in its storage?	Server backup
Usage restrictions	Staff
Usage rights	n/a
Usage frequency	On going
Is the data shared?	No
Who is the data shared with?	n/a
Retention period	Unknown
Comments	

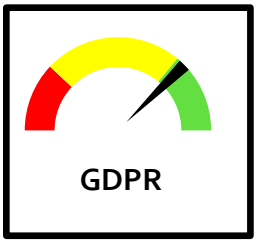
Findings – Data is securely stored – however the database needs cleansing and proper consent will be required to continue relationships with the call group. We would recommend a potential re-permissioning exercise of emails to the Group – We have provided an example already to Fatima from the Macmillan Cancer Charity.



A retention period need drawing up to remove 'old' data.

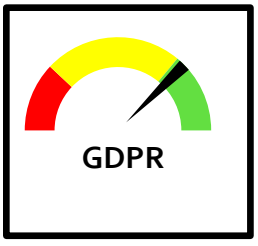
Date of Audit:	19/03/2018
Status of Data	Live
Type of Data	Paper
Description of data	Name/email/company
Employee responsible	Fatima (HHTC)
Date of consent to hold data	Unknown
Where the data is stored?	Server
Source of the data	Webform - downloaded
Purpose of the data	Apply for Grants
How the data is protected in its storage?	In a file
Usage restrictions	n/a
Usage rights	n/a
Usage frequency	n/a
Is the data shared?	No
Who is the data shared with?	n/a
Retention period	Ongoing
Comments	

Findings – Minimal data held and securely stored – **COMPLIANT**



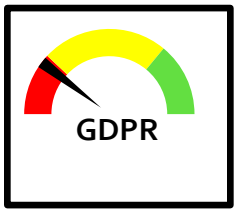
Date of Audit:	19/03/2018
Status of Data	Live
Type of Data	Diary
Description of data	Diary for booking
Employee responsible	Front Desk
Date of consent to hold data	n/a
Where the data is stored?	Diary (Paper)
Source of the data	Counter Applicants or Telephone Call
Purpose of the data	Room Bookings
How the data is protected in its storage?	Under Counter
Usage restrictions	n/a
Usage rights	n/a
Usage frequency	Ad hoc
Is the data shared?	No
Who is the data shared with?	n/a
Retention period	12 months
Comments	

Findings – Minimal data held and securely stored – **COMPLIANT**



Date of Audit:	19/03/2018
Status of Data	Live
Type of Data	Payroll / Pensions
Description of data	Sage 50 Payroll
Employee responsible	Andrew (HHTC)
Date of consent to hold data	On going
Where the data is stored?	'C' Drive on PC
Source of the data	Accounts
Purpose of the data	Payroll & Pension Payments
How the data is protected in its storage?	Back up to USB Stick
Usage restrictions	Just Andrew
Usage rights	Just Andrew
Usage frequency	Monthly
Is the data shared?	Yes
Who is the data shared with?	WSCC Pensions (NI & Name)
Retention period	Ongoing
Comments	

Findings – Sensitive data held on an insecure system due to the backup procedure and an unencrypted system as the local drive is used – this is not part of the HHTC Server backup.



We would recommend finding an alternative secure backup system either to the main server with appropriate encryption.

Date of Audit:	19/03/2018
Status of Data	Live
Type of Data	Purchase & Sales Ledger
Description of data	RBS Software
Employee responsible	Andrew (HHTC)
Date of consent to hold data	On going
Where the data is stored?	Server
Source of the data	Accounts
Purpose of the data	Purchase & Sales Ledger
How the data is protected in its storage?	Server backup
Usage restrictions	Just Andrew
Usage rights	Just Andrew
Usage frequency	Ongoing
Is the data shared?	Yes
Who is the data shared with?	Bank as Processor
Retention period	Ongoing
Comments	

Findings – Minimal data held and securely stored – **COMPLIANT**