West Wycombe Parish

YOU ARE SUMMONED TO ATTEND A MEETING OF THE PARISH COUNCIL TO BE HELD ON THURSDAY 11th JANUARY 2018 AT 8PM IN THE CHURCH ROOM, WEST WYCOMBE

MEMBERS OF THE PUBLIC and PRESS ARE INVITED TO ATTEND

AGENDA

1. To accept apologies for absence
2. Declaration of disclosable pecuniary interests by Members relating to agenda items
3. To confirm and sign the minutes of the previous meeting
4. Report on progress on items in the previous minutes

MEETING CLOSED FOR PUBLIC QUESTIONS
MEETING RE-OPENED

5. Correspondence – see Appendix 1
6. Planning Applications & decisions: None at the time of producing the agenda
7. To discuss any highways issues
8. To discuss the Pedestal Play Area
9. To discuss the burial ground
10. To discuss GDPR – General Data Protection Regulations and consideration of new legislation regarding Data Protection from May 2018
11. To discuss the budget for 2018/2019 and to set the precept
12. To approve the accounts for January 2018 and signing of cheques - appendix 2
13. Members questions
14. Date of next meeting -Thursday 8th February 2018 at 8pm in The Church Room

SHARON L. HENSON, CLERK 4.1.2018

PLEASE REPLY TO: Clerk to the Parish Council, Mrs. Sharon L. Henson,
18, Portway Drive, West Wycombe, Buckinghamshire HP12 4AU
Telephone: 01494 – 448048 Email: clerk@westwycombe.org.uk

Correspondence Received from 14th December 2017 – 4th January 2018

1. Monthly website report – emailed
2. Chilterns Conservation Board newsletter – emailed
3. WDALC agenda – passed to Cllr Mrs Smith
4. Chiltern Society Newsletter
5. WDC Parish Council Tax setting documents
6. Bucks Healthcare – notification of events – on noticeboards
7. NALC Briefing on Data Protection Officers
8. WDC Guidelines for the new Data Protection legislation
9. Thames Valley Police URN - - OCCURRENCE 43170377319 [<AD8335>] – covering damage to basket swing.
10. BCC Invitation Town and Parish Council Conference on 1 February 2018. The focus of the event will be on working together to promote wellbeing in our communities. The conference will run from 09:30 to 14:00.- Do not know where yet.
11. Thames Valley Police Commissioner survey on increasing the precept to cover extra police costs – emailed to Councillors and on website.
12. Information on events for Chalk, Cherries and Chairs project – emailed to Councillors
13. Information on Growing a Rural Community survey
14. Email from a resident about speeding on the Bradenham Road.

Clerks report

1. Basket Swing has been removed and the Handyman will try to repair the original swing. If this cannot be done, then we will make an insurance claim – the second swing was damaged more seriously and may not be reparable.
2. Pedestal Car Park work could not be undertaken due to snow and the frozen surface.
3. Please read enclosed documents on the Date Protection legislation . It is recommended that a data audit is undertaken and privacy notices and notices of data collection must appear on all documentation. As Clerk I have to advise Councillors it is their responsibility to ensure their home computers were up to date with data security eg: Antivirus software, password protected and to refrain from emailing any data which contains personal details. The Clerk has purchased a set of templates for varying applications within the GDPR regulations and has also added a statement to the email address. The Clerk will not be the Data Protection Officer and currently the Bucks Branch of SLCC is investigating ways of dealing with this. We will have to modify and have additional documents for allotments tenancies, grants of exclusive rights for burial, the website ,volunteers, new Councillors and modify some of our policies. See documents enclosed.
4. Please read document on the precept and the budget up to 20th December.
5. Clerk is working with Thames Water and Castle Water re the allotment water – both think they are responsible now!

Appendix 2

Cheques to be paid in January 2018

Mrs S Henson	514.90	December salary
Bucks CC	169.31	January pension
HMRC - online	64.80	Tax/NI
Mrs S Henson	559.78	December exp incl annual working from home allowance
St Lawrence PCC	200.00	Donation to Village Church Loft clock
MH-P Internet	108.00	Annual hosting
Acorn Landscaping	215.83.	9/12 highways grass cutting
The Handyman – James Glasgow	35.00	Removing basket swing
TBS Hygiene	97.20	December collections
John K Lawrence	891.75	¾ burial ground maintenance
Senior Citizens Christmas Party s/o	100.00	Donation
Southern Electricity dd	165.35	Street light energy
Total	**3121.92**	

Statement of Account as at 1st January 2018

Opening balance – 1st November	42586.31
Less December cheques	3194.07
Credit from Castle Water after new meter reading	18.84
Total	**39411.08**

General Data Protection Regulations (GDPR) – EU Legislation (will become law regardless of BREXIT)

This becomes law from 25 May 2018 and replaces the UK Data Protection Act 1998.

This new legislation will be governed by the ICO.

Key Requirements of GDPR – to protect the individual.

- Consent of data subjects for data processing is not mandatory but is encouraged.
- De-identifying (through redaction or pseudonyms) collected data to protect privacy.
- Inform regulatory bodies of data breach
- Safely and securely handling the transfer of data across borders
- The Parish Council will need to appoint a DPO (Data Protection Officer). To oversee compliance. This person MUST fully conversant with all the legislation. There is concern that the Clerk and Councillors are not suitably qualified to undertake this role and may need to be outsourced.

ICO has out in consultation Guidance notes on what needs to be done to audit the data collection. I have attached a copy for your consideration.

Data Protection Officer
WDC has stated that they will not undertake this role on behalf of the Parish Councils.

Website Host
To ensure that the Website host is keeping our data securely we will need a Sharing Agreement. I have emailed MH-P to ask about this.

West Wycombe Parish Council data sources:

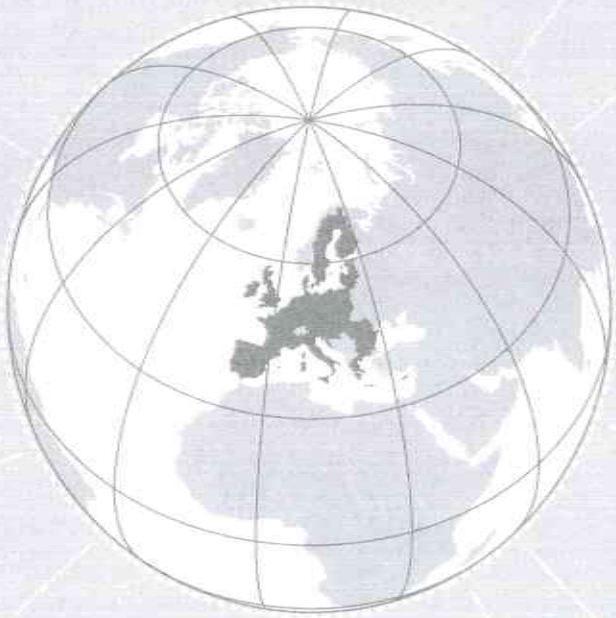
Information	**Stored**
Accounts information	RBS / Computer
Burial Records	Paper / computer
Allotment Database	Paper / computer
Personnel records	Paper /computer
Councillor details	Paper / computer
Planning information	Paper / computer

Preparing for the General Data Protection Regulation (GDPR)

12 steps to take now

ico.
Information Commissioner's Office

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now



1 Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7 Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8 Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9 Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11 Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12 International

If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

ico.
Information Commissioner's Office

ico.org.uk

V2.0 201705

Introduction

This checklist highlights 12 steps you can take now to prepare for the General Data Protection Regulation (GDPR) which will apply from 25 May 2018.

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), so if you are complying properly with the current law then most of your approach to compliance will remain valid under the GDPR and can be the starting point to build from. However, there are new elements and significant enhancements, so you will have to do some things for the first time and some things differently.

It is important to use this checklist and other Information Commissioner's Office (ICO) resources to work out the main differences between the current law and the GDPR. The ICO is producing new guidance and other tools to assist you, as well as contributing to guidance that the Article 29 Working Party is producing at the European level. These are all available via the ICO's Overview of the General Data Protection Regulation. The ICO is also working closely with trade associations and bodies representing the various sectors – you should also work closely with these bodies to share knowledge about implementation in your sector.

It is essential to plan your approach to GDPR compliance now and to gain 'buy in' from key people in your organisation. You may need, for example, to put new procedures in place to deal with the GDPR's new transparency and individuals' rights provisions. In a large or complex business this could have significant budgetary, IT, personnel, governance and communications implications.

The GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. Compliance with all the areas listed in this document will require organisations to review their approach to governance and how they manage data protection as a corporate issue. One aspect of this might be to review the contracts and other arrangements you have in place when sharing data with other organisations.

Some parts of the GDPR will have more of an impact on some organisations than on others (for example, the provisions relating to profiling or children's data), so it would be useful to map out which parts of the GDPR will have the greatest impact on your business model and give those areas due prominence in your planning process.

1 Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation's risk register, if you have one.

Implementing the GDPR could have significant resource implications, especially for larger and more complex organisations. You may find compliance difficult if you leave your preparations until the last minute.

2 Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit across the organisation or within particular business areas.

The GDPR requires you to maintain records of your processing activities. It updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You won't be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

3 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to

complain to the ICO if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language.

The ICO's Privacy notices code of practice reflects the new requirements of the GDPR.

4 Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

The GDPR includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements. If you are geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy. This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who will make the decisions about deletion?

The right to data portability is new. It only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

You should consider whether you need to revise your procedures and make any changes. You will need to provide the personal data in a structured commonly used and machine readable form and provide the

information free of charge.

5 Subject access requests

You should update your procedures and plan how you will handle requests to take account of the new rules:

- In most cases you will not be able to charge for complying with a request.
- You will have a month to comply, rather than the current 40 days.
- You can refuse or charge for requests that are manifestly unfounded or excessive.
- If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.

If your organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. You could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.

6 Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

Many organisations will not have thought about their lawful basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing.

You will also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request. The lawful bases in the GDPR are broadly the same as the conditions for processing in the DPA. It should be possible to review the types of processing activities you carry out and to identify your lawful basis for doing so. You should document your lawful bases in order to

help you comply with the GDPR's 'accountability' requirements.

7 Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

You should read the detailed guidance the ICO has published on consent under the GDPR, and use our consent checklist to review your practices. Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent. Public authorities and employers will need to take particular care. Consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data.

You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

8 Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services ('information society services') to children and relies on consent to collect information about them, then you may need a parent or guardian's consent in order to process their personal data lawfully. The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then you will need to get consent from a person holding 'parental responsibility'.

This could have significant implications if your organisation offers online services to children and collects their personal data. Remember that consent has to be verifiable and that when collecting children's data your privacy notice must be written in language that children will understand.

9 Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Some organisations are already required to notify the ICO (and possibly some other bodies) when they suffer a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.

You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

10 Data Protection by Design and Data Protection Impact Assessments

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

You should therefore start to assess the situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally?

You should also familiarise yourself now with the guidance the ICO has produced on PIAs as well as guidance from the Article 29 Working Party, and work out how to implement them in your organisation. This guidance shows how PIAs can link to other organisational processes such as risk management and project management.

11 Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

You should consider whether you are required to formally designate a Data Protection Officer (DPO). You must designate a DPO if you are:

- a public authority (except for courts acting in their judicial capacity);
- an organisation that carries out the regular and systematic monitoring of individuals on a large scale; or
- an organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions. The Article 29 Working Party has produced guidance for organisations on the designation, position and tasks of DPOs.

It is most important that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to carry out their role effectively.

12 International

If your organisation operates in more than one EU member state, you should determine your lead data protection supervisory authority and document this.

The lead authority is the supervisory authority in the state where your main establishment is. Your main establishment is the location where your central administration in the EU is or else the location where decisions about the purposes and means of processing are taken and implemented.

This is only relevant where you carry out cross-border processing – ie you have establishments in more than one EU member state or you have a single establishment in the EU that carries out processing which substantially affects individuals in other EU states.

If this applies to your organisation, you should map out where your organisation makes its most significant decisions about its processing activities. This will help to determine your 'main establishment' and therefore your lead supervisory authority.

The Article 29 Working party has produced guidance on identifying a controller or processor's lead supervisory authority.

nalc
National Association of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk
w: www.nalc.gov.uk
a: 109 Great Russell Street, London WC1B 3LD

21 DECEMBER 2017

L10-17 | DATA PROTECTION OFFICER

Introduction

Legal briefings L04-17 and L06-17 confirmed that parish councils and parish meetings in England and community councils in Wales are required, under the General Data Protection Regulation (effective on 25 May 2018) and new UK legislation expected next year, to appoint a Data Protection Officer ("DPO").

The purpose of this briefing is to provide more information about (i) a DPO's responsibilities and (ii) the person appointed as DPO.

i) The DPO's responsibilities:

The DPO's responsibilities are as follows.

- to understand the nature, scope, context and purposes of the council's or parish meeting's processing activities and associated risks;
- to be involved in the council's or parish meeting's decisions/activities which have data protection law implications;
- to inform, advise and make recommendations to the council or parish meeting in respect of data protection law compliance;
- to monitor and audit the council's or parish meeting's compliance with data protection law;
- to raise awareness of data protection law with councillors and staff in a council or with the chairman and staff, if any, of a parish meeting.
- to directly report to the "highest management level" (for a council, this would be full council and for a parish meeting, this would mean its chairman);
- to assist the council or parish meeting in carrying out privacy impact assessments when these are necessary;
- to be the contact point for the Information Commissioner's Office (ICO) and for data subjects and
- to be consulted by council or parish meeting if a data breach has occurred.

nalc
National Association of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk
w: www.nalc.gov.uk
a: 109 Great Russell Street, London WC1B 3LD

Notwithstanding the remit of the DPO's responsibilities, GDPR confirms that the council or parish meeting is responsible for compliance with data protection law, not the DPO.

ii) The person appointed as the DPO

L04-17 confirms that the DPO may be an internal or external appointment. In other words, the DPO may be a member of staff or appointed under a service contract. A single DPO may be designated for more than one public authority, taking account of their organisational structure and size. This means a group of councils and parish meetings (or other public authorities such as principal authorities) would be permitted to commission the services of the same DPO or DPO business, provided that a DPO is assigned to each organisation. Leaving the issue of costs aside, a DPO who is a member of staff may be more beneficial than an external appointment, not least because he will be more accessible to the organisation and able to respond to issues as they arise.

The DPO must be appointed on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to perform the responsibilities described in (i) above .

Although a DPO is allowed to have functions or responsibilities additional to those arising from his DPO role, those other tasks and duties must not conflict with the performance of his DPO responsibilities. This means, in particular, that the DPO cannot hold a position which determines the purposes and the means of the processing of personal data. The need to ensure that a DPO can work without conflict of interests is closely linked to the requirement for the DPO to act in an independent manner.

The Article 29 Working Party, which is made up of the regulatory bodies for data protection law which operate in EU member states (and includes the ICO), has produced useful guidance about the DPO. The guidance states:

"As a rule of thumb, conflicting positions may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing."

nalc
National Association of Local Councils

t: 020 7637 1865
e: nalc@nalc.gov.uk
w: www.nalc.gov.uk
a: 109 Great Russell Street, London WC1B 3LD

Can clerks or RFOs be DPOs?

Based on the drafting of GDPR and the guidance from the Article 29 Working Party, it is NALC's view that most clerks and RFOs cannot be designated as a council's DPO. This is because although they may satisfy some requirements of the job, they will not satisfy all of them which are summarised below.

- an absence of conflicts of interests (which may arise from responsibilities as a clerk/ RFO and may include processing activities);
- independence;
- expert knowledge of data protection law and practices and related professional ethics to effectively advise and influence full council and
- adequate time to perform DPO role (many clerks/ RFOs work part-time).

The tool below will help you set your Council Tax for 2018/19. It is constructed on the basis that your share of Council Tax Support Grant (CTSS) will reduce by 13.5%; this is a provisional figure.

Input 1

Select your Organisation using the drop down Box in the Pink Box	
Parish	WestW'- Parish Council

Input 2

Enter either your proposed Precept Demand **D11** or Band D Council Tax for 2018/19 **D13**

Precept	£43,000.00
Or	
Band D Tax	£0.00

Table - Summary of Results *Do not enter data below*

Year	2017-18		2018-19	Difference
Precept	£42,000.00	£	43,000.00	£1,000.00
CTSS Grant	£1,051.52	£	909.56	-13.50%
Income	£43,051.52	£	43,909.56	£858.04
Tax Base	541.13		545.86	4.73
Band D Tax	£77.62	£	78.77	1.48%