WOMBOURNE PARISH COUNCIL

Information security guidelines/ procedures

Acceptable use of information and physical assets

1) Information must **only** be accessed/ used by authorised employees or councillors where there is a justifiable business/ official need to do so.
2) Information must **not** be shared with any other employee or third party unless there is a justifiable business/ official need to do so.
3) Be careful of who is within 'earshot' when discussing people's personal information.
4) Be mindful of telephone callers seeking information about individuals. Be wary of the risk of 'phishing' emails which purport to come from a genuine source seeking information about individuals or that ask you to make a payment. If in doubt always seek to verify the authenticity of the caller or email sender.
5) Do not use your own personal device to process council related personal data.
6) Do not allow any other person (apart from the administrator) to know your password to access any computer system where information is held.
7) Ensure that your password cannot be easily guessed. Avoid names of your children, spouse, partner, etc.
8) Change your password periodically.
9) Do not use the same password for council purposes as you do for personal accounts.
10) Do not use the council's email service for personal communications.
11) Do not use the council internet service for personal use.
12) Employees must not, under any circumstances, download/ install software on to council issued hardware.
13) Non –council issued removable media such as USB sticks must not be inserted in to council computers.

Physical security

1) Entry controls -no one should access the council administration office without authority. Visitors should be collected and returned to reception.
2) Desks and cupboards -employees should, where possible, adopt a 'clean desk' policy. Only that (paper based) personal information that is being worked on at the time should be on an employee's desk.
3) Screens – these should be turned away so that only those people who justifiably need to see information can view it.
4) Overnight procedure- PC's should be shut down at night. Personal information should be filed away, and cupboards kept locked when the office is closed.

Disposal of records

1) Methods of disposal- paper documents that contain personal information should be shredded; electronic records securely erased. Hardware should be erased of all information before disposal.

Transmission

1) Employees should ensure that they have the correct email address before clicking send. If sending documents by post, then addresses should be checked before placing in the post.

Data Processors

These are external organisations the council may instruct to process information on our behalf. If we use a processor then we **must** ensure there is a written contract in place governing the processing. The contract will need to deal with the following matters:

1) the technical and organisational measures they have in place to ensure that there is no unauthorised processing (or loss, damage or destruction) of personal data;

2) that they should not engage another processor without our authorisation;

3) the subject-matter and duration of the processing, its nature and purpose, the type of personal data and categories of employees etc;

4) that they only act on documented instructions from us;

5) that their employees have committed themselves to confidentiality;

7) how between us we will deal with a request for access to their data;

8) what will happen to the data when the processing finishes i.e. is it to be destroyed/ erased or returned to us, and,

9) that they allow us to audit them to see that they do have measures in place to keep employee information safe and that they are complying with those measures.