General

This policy describes our approach to Cyber Protection. It gives rules and guidance for our behaviours on line and using our devices.

Phishing

We will educate everyone not to click on malicious email attachments or website links. Training is the key here.

We will also educate everyone to check any external devices such as drives of any form, before access by virus checking.

Hacking

All of us will keep the operating systems, protection software, and other software we use, up to date with revisions by accepting updates at least monthly but preferably weekly.

All of us will not expose a device that is not protected to public unprotected wifi. This may be by using VPNs.

Boundary Walls and Internet Gateways at Watton and elsewhere

At Watton do not expose our WLP internal systems to outside internet access other than through our own access driven by computers internal to the network seeking access where we have given the user a password.

Where any of us use an outsider to fix a problem by giving them access we will be sure that they are genuinely from that software supplier or our IT support company. We will close the session immediately and delete the software they have used after the session.

Permission will be requested from the user for every piece of software to make changes to any computer or device. Software we no longer use will be uninstalled.

All of us will ensure that the default password for the router will be changed. It will be changed to a strong password (see later). The wifi code for access will be a strong password as well and will be changed from time to time.

Unapproved services, or services that are typically vulnerable to attack (such as Server Message Block (SMB), NetBIOS, tftp, RPC, rlogin, rsh or rexec), will be disabled (blocked) at the boundary firewall by default.

N.B. If a telephone is used only for making calls sending texts and internet use but will not connect to any other device then it need not be password protected.

We will never respond to incoming telephone calls or emails indicating we have system problem.

Access to make alterations through Admin in the WLP Office365 installation will have dual authentication (see below under strong passwords). Our IT service provider has Admin rights to our Office365 installation. We have enabled users to reset their

passwords. Passwords must be changed every 104 weeks. Only Admin can set up guest accounts. We will never transmit passwords unprotected in email.

The user with Admin privileges is the only user to set up new users and delete users or change their access. The user passwords for this are to be kept secure and reviewed at every board meeting being reset at least twice a year.

All devices, computers, laptops used for access and processing must have a firewall installed.

Malware protection

Malware protection software will be installed and enabled on all devices within WLP exposed to the internet, where such devices can be affected by viruses or Malware. It will be kept up to date daily. If a computer has not been in use for a period it will be our first task to ensure the software is up to date before any other use.

The software will be set to scan automatically any downloads or any removable media when connected. Malware software should prompt automatic protection when connecting to potentially malicious sites.

Malware protection software will be configured to scan all the files on the computer every 7 days and a vulnerability scan will be conducted at least monthly. Action will be taken immediately to address issues arising.

Strong passwords

It is recommended that passwords are:

- At least 14 characters. It is recommended that three independent words strung together or a line in a song are used. There are other methods of generating secure passwords that are best used with password vault software such as LastPass.
- In some cases, it can be worthwhile having dual authentication, i.e. you need to have not only the password but also access to a device that will be texted or called e.g. a mobile phone.

Passwords protection on files

Sensitive information is defined as any information about an identifiable person (see Data Protection policy) or where it contains information received in confidence from a client or obtained while working for that client. This will include notes or records taken during discussions before a sale of our services has taken place.

Where a file contains sensitive information about an identifiable person, it will be password protected. Other security may be required see the Data protection policy.

Where the information is not about identifiable persons it will need to be protected only when being transmitted by email.