Local Government for Langton Green, Speldhurst, Ashurst and Old Groombridge

CYBER SECURITY POLICY

An Overview

Where possible, SPC aims to be a standard customer of an Office 365 Managed Service Provider who is set up to handle local council requirements. In our case, as of writing, that is Cloudy IT.

For our CCTV system, we outsource the management and operation of that system to a third party, currently WJ-Sunstone.

Anything IT related which sits outside the purview of these companies should be carefully assessed for suitability.

Customisations to our managed services

- We share a data connection across the CCTV network to the Pavilion building so we can connect our energy monitoring sensors to the internet; this is outside of Sunstone's control. The wireless network emitted is secured to the same level as our standard office Wi-Fi.

Cyber security position

- We aim to remain completely standard customers to companies with strong existing security mindsets.
- We train our Clerks to be cautious of external links and downloads in emails and otherwise online.
- We pay our 365 MSP to create regular backups of our OneDrive, where our documents are stored.
- We ensure all our work is stored in the 365 cloud and synchronised regularly to avoid hardware loss.
- We ensure our owned hardware (laptops, phones) are encrypted at rest and kept up to date.
- The Clerk is the only user in the organisation who should have elevated permissions in 365.
- All accounts in Microsoft 365 have two-factor authentication enabled and enforced. No account can be permitted to log in without two-factor.

Cyber security training

- Our office team should receive Cyber security training refreshers once every two years.

Document procedures

- All our documents are stored in OneDrive, and permissions are split between Councillors and the Office team.
- Councillors only have access to documents they require, which are by rule of thumb those which we would make available to the public on request.

What security risks

- We support BYOD (Bring Your Own Device) for Microsoft 365, so Councillors can log in to 365 on their own unmanaged devices.
- We consider this position to be acceptable as their access to information is limited by our OneDrive organisation outlined above.
- We do not encourage the Office team to make use of 365 on their personal devices due to their elevated permissions within the organisation.
- The 365 account under the most scrutiny is that of the Clerk, as it can take elevated actions. The Clerk shall be aware of this and mindful of login security.
- We must also protect our digital estate – our website and domain name.
    - Our website is via Hugo Fox, a standard provider.
    - Our domain name is managed by Hugo Fox, who is responsible for protecting it, managing the DNS records, and renewing it.

Password Management

- Passwords are currently stored in a protected Office 365 document which only our staff have access to. Access controls to this document are to be periodically checked.
- Passwords are not to be printed out.
- Passwords are only to be shared with those who reasonably require them.
- If a password is suspected to have been shared in error or misused, it must be changed as soon as reasonably possible.

What safeguards

- Our MSP Cloudy IT have built in backups and protections for us against ransomware.
- Full disaster recovery is available through Cloudy IT.

Annual actions

- Ensure our IT position still aligns with this document.
- Ensure owned IT equipment has been receiving updates.