בס"ד

INDEPENDENT JEWISH DAY SCHOOL
an ACADEMY

Cyber Security Policy

Table of Contents

Purpose

This cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure. The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great damage and may jeopardize our reputation as a school. For this reason, we have implemented a number of security measures, prepared instructions that may help to mitigate security risks and offer both in this policy.

Scope

This policy applies to all of our employees, volunteers and anyone who has access, permanent or temporary, to our systems and hardware.

Confidential Data

Confidential data is secret and valuable. Examples of this data in our school are;
-unpublished financial information,

- personal details of families and staff in our school,
- details of prospective families,
- safeguarding information.

All employees are obliged to protect this data and we advise on how to avoid security breaches.

Protect Personal and Company Devices

When employees use their laptops, computers, other digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep their personal and company issued computer secure. They can do this by;
- keeping all devices password protected,
- Use an antivirus software,
- Ensure that they do not leave their devices exposed or unattended,
- Install security updates of browsers and systems monthly, or as soon as available,
- Log into school accounts and systems through secure or private networks only.
- Not accessing internal systems and accounts from other people's devices or lending their own device to others.

New staff to school receive devices that are protected with antivirus software.

Keeping Emails Secure

Emails can contain scams, malicious software and viruses. To avoid these we ask employees to;
- Avoid opening attachments and clicking on links when the content is not adequately explained,
- Be suspicious of titles offering, eg, free advice/prizes,
- Check email addresses and names of people they receive a message from to ensure they are legitimate,
- Look for inconsistencies, eg. excessive punctuation, spelling errors, grammar mistakes.
- To try to communicate only with others within the school g-suite as far as possible and to allow the school office to communicate with others on their behalf.

If an employee is unsure that an email is safe they are advised to not open it and to refer it to our IT support partners.

Manage Passwords Properly

Password leaks can compromise our entire infrastructure. Passwords should be secure and not shared. We advise employees to;
- Choose passwords with at least 8 characters, including uppercase and lowercase letters, numbers and special characters and to avoid easily guessed passwords such as birthdays,etc.
- Remember passwords instead of writing them down.
- To use two step verification where possible,

- Change passwords regularly.

Transfer Data Securely

Transferring data can introduce risk. In order to do so safely, we ask our employees to;
- Avoid transferring sensitive data to other accounts or devices unless absolutely necessary,
- Only share confidential data through the g-suite, not over public Wi-Fi or private connection and always to ensure that it is password protected and encrypted,
- Ensure that the recipients of the data are fully authorised to receive the data and to understand the sensitivity involved,
- Report scams, privacy breaches and hacking attempts.

All reports received are investigated alongside our IT support team, promptly in order to resolve the issue and to send a school wide alert if necessary.

Additional Measures

In general, to minimise security breaches we instruct our employees to;
- Log out of devices and turn off screens when leaving the device,
- Report stolen or damaged equipment as soon as possible to the SBM,
- Change all account details at once should a device be stolen,
- Report a perceived threat or possible security weakness as soon as possible to the IT support team,
- Avoid downloading suspicious, unauthorised, illegal software on school equipment,
- Avoid accessing suspicious websites.

All staff, pupils and parents also comply with our acceptable user policy.

IT Support

Our IT support team at Joskos should;
- Install firewalls, antivirus software and access authentication systems,
- Provide security training to all staff,
- Inform staff of new scam emails and viruses and ways to combat them,
- Investigate breaches thoroughly.

Remote Working

As employees might be working from home at times, they must adhere to this policy in the same way. They must follow all data encryption, protection standards and settings and ensure that their private network is secure. Advice can be sought from our IT support team.

Disciplinary Action

We expect all of our employees to always follow this policy and those who cause security breaches may face disciplinary action. This action may take the following form;

- First time, unintentional, small scale security breach may result in a verbal warning and a training session on security.
- Intentional, repeated or large scale breaches may result in more severe disciplinary action up to and including termination of contract.
- All situations will be assessed on a case by case basis.