ICT & Digital Services for Schools

Secure Email Policy

2022-2023

Bitz 'n' PC'z Ltd
computer repair and IT consultancy

At Bitz ‘n’ PC’z Limited, we take the security of your data very seriously. One way we can do this is to encrypt messages that we send you via email if it contains sensitive information. This means that only you will be able to open and read the email.

From March 2022, we are using a company called Zivver to send our emails securely.

If we need to email you with any information that we consider confidential then there are a few extra steps you will need to take to open the email.

Your email will contain a link to a secure website where you can access the message. On the website you will be prompted to request a code via a text message (if your mobile number is known to us), known as an SMS code. Once you have received this code via text you enter it into the website and this will then show you the message.

How to read a message that was sent via Zivver

Did you receive an email from Bitz ‘n’ PC’z Ltd via Zivver? If so, you can open this message by clicking the button that says ‘Open Message’. When you do, the secure Zivver website will automatically open.

If you have received a message that is secured with an SMS (or text message code), click on the ‘Request code’ button. Insert the code that you have received and you can now read the message. You can read the articles on Zivver's help page for more information about how to read a secure message.

Opening a message with an email code

In some instances, we may send an email code instead of an SMS/text code. You will be prompted to check your email for the code, and then you can enter it into the website and read the message.

Want to respond to an email that was sent via Zivver?

If you want to reply to an email message that was sent via Zivver, you can click on the 'Reply' button on the webpage where you are reading the message.

You can type your message in the text window. You can also add attachments if needed using the ‘Add attachments’ (paper clip) button. Click ‘Send’ to send your reply. When the recipient of your message responds, you will receive another notification message.

More about Zivver

Zivver allows you to send emails and exchange files securely. Zivver encrypts messages with sensitive content, such as personal data, files, reports, or other information you want to send securely. If you send a message via Zivver, it is guaranteed to be safe. This means that no one but the sender and the recipient have access to the message. Not even hackers. Additionally, Zivver uses smart technologies to prevent Bitz ‘n’ PC’z Limited’s users from sending sensitive information to the wrong recipient.

Questions?

Do you have questions about an email you received? Zivver have support pages you can use, or you can email them: support@zivver.com.

If you want to know more about Zivver: https://zivver.com.

Bitz 'n' PC'z Limited manages your information in line with the Data Protection Act 2018 and General Data Protection Regulation 2016/679.

The use of Zivver adds a layer of security to the information contained within any email communication you have with Bitz 'n' PC'z Ltd. Your rights under data protection law are not impacted by the use of Zivver. Please contact our Data Protection Officer if you have any questions about how we use or process your information.

The technical bit!

As a SaaS solution, Zivver services are hosted on an AWS Virtual Private Cloud across multiple ISO 27001 and SOC II certified data centres within the European Economic Area (EEA).

The main application is hosted using AWS ECS to provide a highly available and scalable architecture. Multiple instances of the application are typically available at any time, distributed over three availability zones to ensure high levels of resilience. The system's databases are hosted using AWS RDS with master and replica databases located in two different AWS availability zones. The architectural design allows for automated failover in the event of a single datacentre outage.

Emails in transit are protected with TLSv1.3 (TLSv1.2 still supported). At rest storage uses a combination of RSA for asymmetric encryption and AES GCM (authenticated encryption) for symmetric encryption. The key strength of the utilised encryption protocol depends on what is supported by the client where at least TLS 1.2 must be used in transit (we support TLS 1.3 also). Minimal key strengths for RSA is 2048 bits, for AES is 128 bits and ECC 256 bits. Zivver has a strict Zero-Knowledge policy. As a result, it is demonstrably not possible for Zivver to view the content of messages or access them because Zivver does not store a key or derivative in order to be able to decrypt messages.

Highly confidential data like the personal data of our customers is encrypted at rest. Only the customers have access to the keys to decrypt this data in a BringYourOwnKey principle. As a result, it is not possible for Zivver to view the content of any messages.