

Advantage Learning Technologies (Pty) Ltd – Security Policy



June 2019 | Version 2.1

1. Introduction

There is no such thing as “perfect security”. We have to compromise between increased levels of security and the convenience to you in transacting with us.

2. Our security responsibilities

We will ensure that:

- we host our website in a secure server environment that uses a firewall and other advanced security measures to prevent interference or access from outside intruders.
- the information (this is limited to information relating to payments like credit card or payment information) you give to us that is stored on or passes through our systems is protected. Encryption is used to protect the personal information you give us. This includes using your credit card on our website (see below).
- the links from our systems to systems under the control of third parties (for example our payment gateways) are secure.
- regular backups of data are performed to ensure it can be recovered in the case of a disaster.
- we take reasonable steps to secure your payment information and use a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of the transaction concerned.

3. Our security disclaimers

Please note the following:

- The third parties whose systems we link to are responsible for the security of information while it is collected by, stored on, or passing through the systems under their control.
- We will use all reasonable endeavours to ensure that our website and your information is not compromised. However, we cannot guarantee that no harmful code will enter our website (for example viruses, bugs, trojan horses, spyware or adware). You should be aware of the risks associated with using websites (addressed below).
- If you experience a problem or loss that is caused by information you provided to us, your computer being compromised in some way or by something beyond our control, we cannot take responsibility for causing the problem. We will, however, do our best to help you if we can.

4. Your security responsibilities

4.1 **Recommended steps.** You should:

- Install and activate appropriate security software on your computer. This should include anti-virus, anti-spyware and anti-spam software.
- Run regular scans of your computer for viruses.
- Update your security software to ensure you are always running the current version.

4.2 **Additional steps.** Other steps you should take to help protect your computer include:

- Check your Internet browser’s security settings for ways to make your browsing more secure.
- Make sure that you have entered secure pages when filling in your credit card details. Look for a small yellow lock commonly seen at the bottom right of your browser and http changes to https on the address bar.
- Sign out after you have transacted electronically.

5. Protecting your password

You should:

- Never share your password with anyone.
- Never send your password via email.
- Make your password as strong as possible.

6. Credit card information

6.1 **Safe and secure.** Transacting with us electronically (including transacting and using your credit card on our website) is safe and secure. It is much the same as transacting in person face-to-face.

6.2 **Payment processing.** We do not get involved in any credit card transactions directly. All credit card transactions are handled or acquired for us via our payment gateway who are the approved payment gateway for our bankers. Only your customer details (such as your name, email address and contact details) are stored on our site. No credit card details are stored on our website. Our payment gateway uses the strictest form of encryption, namely Secure Socket Layer 3 (SSL3). No credit card details are stored on the payment gateways website. You may go to their website to view their security certificate and security policy.

6.3 **Payment verification.** A Certificate Authority (or CA) checks, verifies, and certifies our service provider’s company registration documents and domains to ensure that nobody can impersonate them to obtain your payment information.

- 6.4 **Secure URL.** Our website has SSL verification. This means that when you access our website the URL will be “https”. This is indicative of a secure Internet transaction.
- 6.5 **Verification programs.** We currently support the [Verified by Visa program](#) and the [MasterCard SecureCode](#). You can use your Visa or MasterCard credit card as payment for an order, you will be asked to enter your 3D Secure verification passwords/OTP's (Verified by Visa password or MasterCard SecureCode) on checkout.
7. **Transaction currency**
- 7.1 **Currency.** We use the Rand (ZAR) as our transaction currency. All our payment options are presented in Rands(ZAR).
8. **Phishing**
- 8.1 **Secure URL.** You must only log in to your account from a page that begins with <https://advantagelearn.com/>
- 8.2 **No confirmation through links.** We will never ask you to confirm your username and password or other sensitive information by clicking on any links in an email other than the email link we send you at registration to verify your email address. Be aware of “phishing” attacks where criminals attempt to obtain your sensitive information by sending you an email, masquerading as an email from us, asking you to access your account or verify information via links in the email, or diverting you to a fake Advantage Learn website. Please report any suspected phishing attacks to us immediately to prevent any harm to you or other users.
9. **Contact us**
- You must report any suspicious or unauthorised activity relating to your use of <http://www.advantagelearn.com/> by contacting us. This will help us make our website as secure as we can.
10. **Our right to take action**
- We reserve the right to take whatever action we may deem necessary at any time to preserve the security and reliable operation of our system. You undertake not to do (or permit anything to be done) that may compromise the system under our control.