Company Credit Card and Anti-Fraud Policy

INTRODUCTION

This policy sets a framework for using the company credit card on behalf of Collaborate (the Company), outlines the Company's stance against fraud and provides guidance on how to recognise and report fraudulent activity. The Company is committed to maintaining the highest standards of integrity and ethical behaviour in all aspects of its business operations. The company credit card will be subject to strict terms and conditions of use as well as controls.

- To ensure good financial management, the company credit card[s] will only be issued to Authorised Cardholders.

- All Authorised Cardholders are responsible for ensuring that these policies and procedures are complied with to ensure the company credit card is used appropriately and the company finances are safeguarded, in line with the Expenses Policy.

- Authorised Cardholders will be required to sign a declaration to confirm that they will adhere to this Company Credit Card and Anti-Fraud Policy.

AUTHORISED CARDHOLDERS

Cards will be issued on a case-by-case basis and must receive the approval of the Department Head. Authorised Cardholders are responsible for ensuring the security and safekeeping of the company credit card[s] issued to them as well as the related PIN number and other security details.

It is the Authorised Cardholder's responsibility to ensure appropriate use of the company credit card they hold. The Authorised Cardholder should familiarise themselves with the Company's business expenses policy and must ensure that the company credit card[s] are not used for transactions which are not appropriate.

Any Authorised Cardholder who leaves the employment of the Company or otherwise ceases to be authorised as a cardholder, for whatever reason, shall return their company credit card to the Finance Director or Finance Manager, at the earliest possible opportunity. The finance department will contact the card provider to cancel the company credit card and remove the previously Authorised Cardholder from the Company's account.

CARD SECURITY

The Authorised Cardholder is responsible for the safekeeping of their company credit card.

The Authorised Cardholder is responsible for custody of the card details and security information and to guard against possible fraud.

If a company credit card is lost or a PIN number is forgotten or compromised, the Authorised Cardholder must inform the card provider and Finance Director or Finance Manager, immediately.

The contact number for reporting lost or stolen cards to the card provider are;
Amex: 0800 917 8043
Barclaycard: 0800 008 008
Pleo: use app to freeze or cancel card.

In the event of any suspected fraudulent use of the company credit card, the Authorised Cardholder must advise their Department Head, Finance Director and Finance Manager as soon as they are aware of any possible fraudulent use. If this happens outside of normal working hours, the Authorised Cardholder must immediately advise the card provider.

ONLINE SECURITY

When transacting online, it is important to be aware of internet security precautions that can be taken and make sure that the website being used can be trusted. Aspects that indicate a website should be able to be trusted include:

- Web address should always begin with https:// as the 's' indicates the website is secure.
- Closed Padlock or Unbroken Key icon in address bar or browser window indicates that the site is enabled and encrypted for online safety.
- Even more secure sites use extended validation certificates, which in more modern web browsers turn the address line green.

FRAUD PREVENTION

All staff will receive fraud training on the first day of their induction, and also prior to being given the Company credit card. Even if you do not have a Company credit card, you must be aware of fraudulent activity and prevention, and adhere to the same checks if spending your personal money and then submitting an expense claim. There will be follow up training or email reminders and warnings to all Authorised Cardholders on recognising the signs of fraud and the importance of reporting any suspicious activities.

The Company will maintain open channels of communication to encourage employees to come forward with any concerns or suspicions related to fraud. Anonymity and confidentiality will be maintained as much as possible.

Fraud tactics are becoming increasingly sophisticated, and it is often incredibly difficult to differentiate between scams and legitimate requests. We have recently seen a rise in email scams, whereby an email looks to have been sent by the MD or a colleague asking for you to buy something, an Apple voucher for example, or specific items. Before using the company credit card, you must check that this is a legitimate request, ideally using a secondary channel of communication – for example, if the request has come via an email, it would be sensible to call that person or speak to them face to face to check it was really them that asked for it. If you are unsure or a second authorisation is not possible, do not proceed. Notify the Department Head, Finance Director and Finance Manager of any requests that you feel are not genuine.

Never give out access codes or codes received via a 2-point authentication service, even if the person claims to be working on behalf of or for a bank.

Stop – Take a moment to stop and think before committing to a request or providing certain details.

Challenge – Could it be fake? It's ok to challenge a request, ignore it or refuse. Only criminals will try to rush or panic you.

Protect – Report any fraudulent activity immediately. If you think you have been a victim of fraud, you must report it to your Department Head, Finance Director and Finance Manager.

INVESTIGATION

Upon receiving a report of suspected fraud, the Company will conduct a prompt and impartial investigation. The investigation will be carried out by competent individuals.

All investigations will be documented, and relevant evidence will be preserved.

The company reserves the right to deduct any fraudulent activity from your salary if the appropriate fraud prevention steps above have not been taken.

CREDIT CARD LIMITS

There is an overall credit limit attached to the Company's Credit Card Account.
Each Authorised Cardholder will have individual card limits which will be advised at the time of issue.

If an Authorised Cardholder becomes aware of a need to request a temporary increase in their credit limit for a specific purpose, then they should contact the Finance Manager as soon as possible in order to allow time to manage our overall credit limits appropriately. The request must be accompanied by a brief explanation as to why the increase is required.

ACCEPTABLE USE

Company credit card usage is intended to facilitate transactions only in appropriate circumstances, such as to primarily provide an easier means of booking and paying for travel and accommodation in connection with official Collaborate purposes.

The company credit card must only be used for permitted expenditure. The Authorised Cardholder has permission to execute permitted expenditure in person using the PIN number for authorisation, via telephone transactions and via online transactions.

The company credit card may be used for:

- accommodation bookings or payment
- payment of travel costs
- payment for meals and hospitality in line with our expenses policy
- purchasing essential materials on site
- team culture events in line with the company budget

The company credit card must not be used for:

- withdrawing cash
- the purchase of unauthorised goods
- purchase of meals etc outside of our expenses policy

These lists are not exhaustive, if you are unsure please contact your Department Head, Finance Director or Finance Manager.

The company credit card must not be used for any type of personal expenditure as expenditure of the company credit card must only be for business use.

Should the Authorised Cardholder use the company credit card for any purpose other than business expenses, the Authorised Cardholder will be required to repay the amount charged to the company card.

Authorised Cardholders will be required to sign the Credit Card and Anti-Fraud declaration to confirm that they will consent to the Company making deductions from their salary or any other payments owed to the Authorised Cardholder, to recover this amount.

The Company reserves the right to withdraw the company credit card from any Authorised Cardholder if they fail to comply with any of the terms and conditions of this policy, or for any other reason the Company sees as an acceptable reason to withdraw the company credit card. Authorised Cardholders may have their company credit card withdrawn temporarily if they are subject to disciplinary investigations and procedures.

If there are any questions or enquiries about acceptable use of the company credit card[s] please contact the Finance Director or Finance Manager.

MONITORING USE AND RECORD KEEPING

Authorised Cardholders are responsible for ensuring that appropriate record keeping is maintained for their company credit card. It is essential that evidence for each transaction is collected and stored safely to meet accounting, VAT recovery and internal control requirements.

The Authorised Cardholder will be responsible for providing details of each occasion of use and for submitting receipts or vouchers for all expenditure. Any expenditure for which supporting receipts or vouchers are not presented will become the liability of the cardholder.

Further information
If there are any questions or enquiries about this policy and its application, please contact NAME.

Monitoring and review of this policy
Collaborate will regularly monitor the effectiveness of this policy, to ensure the policy works in practice. We will provide any relevant information or training if any changes are made to this policy.

Credit Card and Anti-Fraud Declaration

Name:
Job title:
Department:

I confirm that I have read and understood Collaborate's Credit Card and Anti-Fraud Policy, as well as the separate Expenses. I confirm that I will adhere to all points within this policy, in my use of the company credit card provided.

I confirm that I will, as soon as is practicable, report a lost or stolen company credit card to the Card Provider and the Finance Director or Finance Manager. I will also report any fraudulent or any suspected fraudulent activity to the Department Head, Finance Director and Finance Manager in line with the credit Card and Anti-Fraud Policy.

Should I use the card for any purpose other than business expenses incurred, I accept to repay to Collaborate, the amount charged for this purpose. I also consent to Collaborate making deductions from my salary or any other payments due to me, to recover this amount.

Signed:

Date: