| | |
|---|---|
| **Purchase Cards Policy** | |
| Security Classification | **OFFICIAL** |
| Disclosable under Freedom of Information Act 2000 | Yes |

| | |
|---|---|
| **POLICY TITLE** | **Purchase Cards/ Force Credit Cards** |
| REFERENCE NUMBER | **WMP161** |
| Version | **1.1** |

| | |
|---|---|
| **POLICY OWNERSHIP** | |
| DIRECTORATE | COMMERCIAL SERVICES |
| BUSINESS AREA | FINANCE |

| | |
|---|---|
| INITIAL IMPLEMENTATION DATE | **May 2021** |
| LATEST REVIEW DATE | **September 2023** |
| NEXT REVIEW DATE: | **September 2025** |
| RISK RATING | **MEDIUM** |
| EQUALITY ANALYSIS | **LOW** |

West Mercia Police welcome comments and suggestions from the public and staff about the contents and implementation of this policy. Please e-mail polciesandprocedures@westmercia.police.uk.

**POLICY IDENTIFICATION PAGE**

This policy covers the use and terms of conditions of Force issued Purchase/ Credit Cards.
This policy should be read in conjunction with:

- Financial Regulations
- Police Regulations (re discipline)
- Support Staff Handbook (re discipline)
- Travel & Subsistence Policy
- Card Holder Agreement & Guide

## 1.0 PURPOSE OF POLICY

The aim of this policy is to establish a clear understanding of the Terms and Conditions of use when issued with a Force Purchase/Credit Card. Users of these cards should be aware that failure to comply with this policy may result in an investigation by Internal Audit or the Professional Standards Department. This policy will enable you to make the best use of your Card, understand your obligations and restrictions, and will also advise you of what to do and who to contact if you experience any problems

## 2.0 POLICY OUTLINE

This policy informs Police Officers and Police Support Staff on how and when a card should be used.

This policy will deal with:

1. Cardholders Responsibilities
2. Line Managers Responsibilities
3. Lost and Stolen Card
4. Misuse of card
5. Security of the Card
6. Loyalty / Reward Points
7. EBay Purchases
8. PayPal Accounts
9. Amazon Accounts
10. Travel/ Hotels and Subsistence
11. Damaged Cards
12. Continuation Cards
13. Dormant Cards
14. Revoked Cards
15. Maternity/paternity Leave, Long Term Sickness, Career Breaks, Secondments
16. Spending categories
17. Spending Limits
18. Telephone Orders
19. Embedded Card
20. Damaged Goods
21. Internet purchases

22. Disputes/ Errors

## 2.1 Responsibility of the Cardholder

It is essential for each Cardholder to maintain a record of their transactions each month which can then be used by the Cardholder to populate the monthly Purchase Card Statement on HSBC Mivision to ensure an accurate record of the spend. You will receive an email notification from HSBC to advise you that your statement is now available on Mivision.

It should be noted that Banks and Vendors can make mistakes and failure to reconcile transactions against the monthly statement could allow fraudulent transactions to remain undetected or expose the Authority to financial losses (as well as resulting in incorrect expenditure being charged to departmental budgets).

To enable reconciliation, the Purchase Card statement should be checked to ensure that:

- all goods and services detailed on the statement have been received and are recorded
- there are no erroneous entries on the statement - erroneous entries must be reported immediately to the line manager and the Financial Accounting Team.
- the amounts charged on the statement match the receipt/invoice which must also be uploaded to HSBC Mivision.

Where receipts / invoices are missing, it is still the cardholder's responsibility to check and approve the expenditure. The Cardholder should contact the relevant vendor to obtain any necessary receipts / invoices for VAT reclaim purposes. The Cardholder will need to email Financial Accounting to explain any missing receipts or invoices.

**Repeated failure to submit receipts or invoices will result in a warning from the Financial Accounting team, copying in the cardholder's line manager. Continued failure will result in removal of the purchase card and a referral to Professional Standards where a formal disciplinary investigation may take place.**

The coding and uploading of spend on Mivsion must be completed within 10 working days of receiving the statement. If the Cardholder is unable, for any reason, to complete this action, the Cardholder must email the Financial Accounting Team.

## 2.2 Responsibility of the Line Manager

- To read and be familiar with the Purchase Card Policy.
- Ensure the Cardholder fully understands their responsibilities with regards to the use of the Purchase Card
- To keep the Financial Accounting Team informed of staff changes / leavers or any other issues.
- Ensure that all transactions are in keeping with the Cardholder's responsibilities and are charged to appropriate Cost Centres.

- Where a personal transaction is made in error, to ensure that the value of the transaction is promptly refunded to the Force, report the error to the Financial Accounting Team and Professional Standards if necessary for investigation if appropriate to do so and remind the Cardholder of their responsibilities.
- To ensure that damaged Purchase Cards are replaced.
- To submit any requests for changes to single transaction limits and / or monthly transaction limits as and when necessary to the Financial Accounting Team by email.

### 2.3 Lost or Stolen Cards

If it is discovered that a card has been lost or stolen or the number has become known to a third party who may use it fraudulently, the Cardholder must immediately contact the card provider on 0345 6015 934. This service is available 24 hours a day, 365 days a year. Failure to report this leaves the Force vulnerable to fraud. The Cardholder must also inform, no later than the next working day, the Financial Accounting Team, financialaccounting@westmercia.police.uk or 01905 716208 or 01905 716215. The Financial Accounting Team can arrange for a replacement card to be issued. If a previously reported lost or stolen card is subsequently found, it must be cut it in half and returned to the Financial Accounting Team. Failure to report this within the timeframe stated may result in the Cardholder having their card privilege rescinded.

### 2.4 Misuse of the Card

Use of the Purchase Card will be subject to regular and comprehensive audit. Any deliberate misuse will result in the card being withdrawn. Deliberate misuse will be deemed to be a disciplinary offence and will be referred to Professional Standards. Such misuse may include, but is not limited to, the following:

- Making, or attempting to make, purchases at non-approved vendors.
- Purchase of goods for non-business use.
- Giving the card or card number to another person or using another person's card or card number.
- Using the card for personal purchases

Repeated 'accidental' personal purchases may also be considered deliberate misuse and will be subject to the same referral to Professional Standards.

### 2.5 Security

Cardholders must take all reasonable precautions to prevent loss or misuse of the Purchase Card or any of the details on it. The following precautions are required by Cardholders:

- Sign the card immediately upon receipt.
- Do not allow any other person to use the card. Treat the card like cash – never leave it unattended.

- Keep the card, the card number, the card security code, PIN number and security details such as Cardholder's date of birth and mother's maiden name (memorable name) secure.
- Never give card details over the telephone to anyone other than a bona fide vendor – no person or organisation will ever contact a Cardholder asking for card details but there are fraudsters who might try to obtain your details in this way.
- Cards must not be kept in desks or cupboards etc.
- Cardholders should not change the PIN of the card to 'match' or be the same as their own personal cards.

Cardholders are responsible for all purchases made on their cards and must be able to account for all usage of the card. Allowing third parties to use the card on their behalf is strictly prohibited as it exposes the Force to risk and potential for fraud. If it is determined that a Cardholder has allowed a third party to use the card on their behalf, a referral will be made to Professional Standards and their card privileges may be revoked.
In the event that a Cardholder no longer needs a card, or they are due to leave the force, on the last day of use the card must be cut in half and returned to the Financial Accounting Team who will cancel the card at the Bank making it invalid.

### 2.6 Loyalty Reward Cards

The use of loyalty cards to obtain points when making purchases on behalf of the Force is strictly prohibited.
A Cardholder may be warned in relation to the collection of points, but persistent abuse will result in the Purchase Card being revoked and Professional Standards informed.

### 2.7 EBay Purchases

The use of EBay to make purchases is strictly prohibited unless it is operationally vital for this purchase to be made. A retrospective explanation will be required.

### 2.8 PayPal Accounts

The use and setting up of PayPal accounts for making purchases on behalf of the Force is strictly prohibited.
Use of a PayPal account will result in a referral to Professional Standards.

### 2.9 Amazon Accounts

Under no circumstances should a Cardholder create an Amazon Account for use on behalf of the Force.
Under no circumstances should a Cardholder save their Purchase Card details to their own personal Amazon Account. If a purchase is to be made via Amazon, the Cardholder must ensure that the card details are deleted post-purchase to ensure no 'accidental' personal purchases.

### 2.10 Travel / Hotels and Subsistence

Purchases for travel and hotels is prohibited, except in exceptional circumstances. Otherwise, these purchases are to be made via the elected provider e.g., Click Travel.

Purchases for travel are only permitted where the travel:

- is of operational importance
- and takes place within 7 days (which would mean a conventional request would not be completed in time)
- and falls within the cost parameters set out in the Travel and Subsistence Policy

It is vital that travel-related purchases are submitted through the correct channels to allow the Force to renegotiate appropriate contracts.

Cards are not to be used for subsistence except for operational reasons. Normally subsistence would be paid for by the individual and reimbursed via the Mercury Payroll System.

### 2.11 Damaged Cards

If a card becomes damaged, the Cardholder should inform the Financial Accounting Team who can then order a replacement card. The Cardholder is required to cut the damaged card in half and return it to the Financial Accounting Team

### 2.12 Continuation Cards

Replacement cards are issued every two years, and this will normally be 28 days in advance of the card's expiry date**.** On receipt of the new card the Cardholder must immediately sign it on the reverse and securely destroyed the old card.
If the replacement card does not arrive 28 days in advance of the expiry date, it is the Cardholder's responsibility to contact the Financial Accounting Team to notify them.

### 2.13 Dormant Cards

Cardholders who have not used their cards within a 6-month period will be written to by the Financial Accounting Team to advise them of the intention to rescind the card privileges. Should the Cardholder wish to contest this, they must submit their explanation for the retention of the card, with their Line Manager's support, within 14 days of the notification to cancel.

### 2.14 Revoked Cards

The Force reserves the right to revoke the card immediately should it be found that the cardholder has breached the Purchase Card Policy. Cardholders who have had their card revoked will not be reissued with another card and the circumstances of the revocation will be referred to Professional Standards.

### 2.15 Maternity/Paternity Leave, Long Term Sickness, Career Breaks, Secondments

It is the Cardholder's responsibility to securely return their card for cancellation whilst on Maternity/ Paternity Leave, Long Term Sickness, Career Break or Secondment. When the cardholder returns, they must apply for a new card.

### 2.16 Spending Categories

The Purchase Card must not be used to purchase goods or services which are not appropriate to the needs of the service area where it is being used. Therefore, certain categories of spend will be "blocked" in line with Corporate and Departmental policy.

Should Cardholders encounter problems using the card due to a vendor being in a "blocked" category, the Cardholder should contact the Financial Accounting Team who have the authority to amend any categories associated with the card. The card provider will inform the Force each time an attempt is made to make a purchase from a "blocked" vendor.
Repeated attempts to make purchases from a "blocked" vendor, without contacting the Financial Accounting Team, may be treated as deliberate misuse and subject to that procedure.

### 2.17 Spending Limits
Each Cardholder has a single transaction limit and an overall monthly credit limit - both of which will have been set by the Financial Accounting Team in conjunction with the Line Manager.
If a Cardholder attempts to make a purchase that exceeds either of these limits the bank will decline the transaction. The limits are set for security purposes and need to be neither too low nor too high. If a Cardholder needs the card limit to be increased or decreased, their Line Manager should approval the increase and submit a request to Financial Accounting. If a transaction fails to be accepted (is declined) and the Cardholder believes the transaction should have been accepted, the Cardholder should contact the Financial Accounting Team, who will find out what the problem is. The Financial Accounting Team will need written authorisation either from the Line Manager or relevant Budget Holder.

### 2.18 Telephone Purchases
*(Also known as Cardholder Not Present or CNP Transactions)*

CNP is the name given to any transaction where the Cardholder is not present in person at the vendor's premises and is a common term applied to Mail, Phone and Internet purchases.

Cardholders may be asked for the following information when conducting a CNP transaction (i.e., if ordering by telephone or over the Internet):

| | |
|---|---|
| Cardholder Name | the Cardholder name as it appears on your card |
| Card Number | As it appears on the card |
| Card Expiry Date | As it appears on the card |
| Customer Reference | This is only required if it is necessary to override the default codes that will be generated by making the transaction. |
| Delivery Address | Under no circumstances must the Cardholder give their home address or a non-Force address for delivery purposes. For verification purposes the address given should always be the Force's address (usually the address |

| | |
|---|---|
| | shown on your statement). The delivery address can be different. |
| Card Security Code | This must be quoted only if the vendor asks for it as an additional security check. It is the last three digits of the number printed in the signature panel on the back of the card. The security number should not be divulged to any other third party under any circumstances. |

The details given will be used as part of the Bank's authorisation processes so they must be accurate, or the transaction may be declined.

### 2.19 Embedded Cards

Embedded card arrangements are put in place as part of the procurement process with specific suppliers who supply large volumes of low value goods. Where such arrangements exist, they should be used by all cardholders for all appropriate spend.

Monthly transactions will be extracted from the card provider's web site by the Financial Accounting Team. The Finance Systems Team will upload the transactions into the finance system to create the payment and the appropriate accounting entries. Charges will be reviewed by budget managers.

### 2.20 Damaged Goods

It is the Cardholder's responsibility to contact the vendor to arrange for the goods to be either replaced or returned. If the goods are returned, the Cardholder should instruct the vendor to CREDIT the Purchase Card Account. Enter the CREDIT details on your Transaction Log and use the same Cost Centre and General Ledger codes as on the original transaction.

### 2.21 Internet Purchases

Only use your Purchasing Card to purchase online from organisations that have physical premises and/or places that have been around a while and have been conducting online transactions for some time without major problems.
The Cardholder must never enter their card details over an unsecured site. A secure site will use encryption to protect the Cardholder's data as it travels between the Cardholder's computer and theirs. A secure site with have http:// in the page address which changes to https:// and / or a little closed lock icon appears in the lower portion of your web browser.

**Cardholders must never send the card details via email.**

### 2.22 Disputes or Errors

It is the Cardholder's responsibility to identify incorrect entries on their statement (either quantity or price) and to contact the Vendor in case they have made an error. If a credit is required, the Vendor should be instructed to make a credit on the Purchase Card account. If the Cardholder is not satisfied with the Vendor's response, the

Cardholder must contact the Financial Accounting Team at the earliest opportunity who will take any necessary action.

## 3.0 IMPLICATIONS of the POLICY

Consider other implications of the policy and make comment **only** in those areas of significance. The following **must** be considered:

- Code of Ethics
  We have considered and included any code of ethics implications in the Policy.

- The Standards of Professional Behaviour
  The Policy sets out the expected standards of professional behaviour required from a Cardholder and any breach of these will be reported to Professional Standards as detailed above.

- Code of Practice on the Management of Police Information
  There are no specific issues arising as a result of implementing this policy.

- Risks / Health and Safety considerations
  There are no specific health and safety issues arising as a result of implementing this policy.

- Human Rights / Equality / Data Protection / Freedom of Information
  There are no human rights, equality, data protection or freedom of information issues arising from the implementation of this policy.

- Legal considerations
  There are no legal issues arising from the implementation of this policy.

- Financial Implications
  This policy supports the PCC’s Financial and Contract Regulations regarding the proper accounting for expenditure.

- Implementation requirements (an implementation plan should be included where necessary)
  To be implemented with immediate effect.

## 4.0 CONSULTATION

| ***Chief Officer/Business Lead Consulted*** | ***Date Authorisation Received*** |
|---|---|
| Mike Kaine, Financial Accounting Manager | April 2021 |
| Pippa Wilkinson, Financial Accountant | July 2023 |
| Jamie Barker, Financial Accountant | July 2023 |

| | |
|---|---|
| Rachel Adie, Head of Finance | July 2023 |

## 5.0 DOCUMENT HISTORY

The history and rationale for change to policy will be recorded using the below chart:

| Date | Author / Reviewer | Amendment(s) & Rationale | Date of Approval / Adoption |
|---|---|---|---|
| | | Previously approved at JNCC meeting | JNCC 10/05/2017 |
| July 23 | Jo Horton/ Niamh Larkin | Update and re-write to reflect the latest processes – minor changes v1.1 | July 2023 |

## 6.0 PROCEDURE

A procedure document is available separately.

## 7.0 ASSESSMENT AND ANALYSIS

This policy has been subject of an Equality Analysis available on a separate document.

## 8.0 MONITORING / EVALUATION

The Monitoring and review of this procedure is the responsibility of the procedure owner.