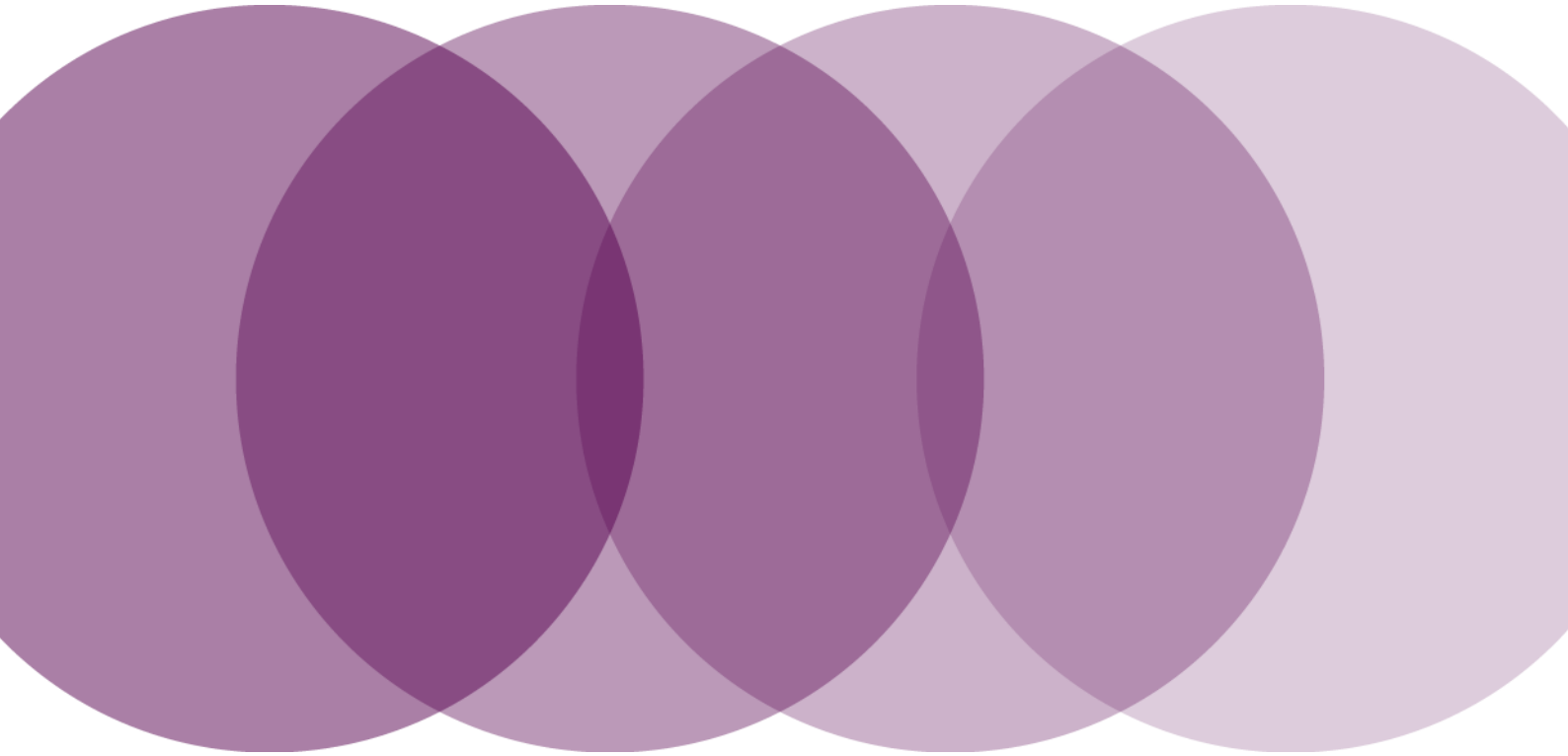
Ministry of JUSTICE | Procurement

Government Procurement Card (GPC) Policy



September 2012

Alternative format versions of this report are available on request from procurement.compliance@hmps.gsi.gov.uk

Contents

Glossary of terms

Glossary term	Glossary definition
Business Area	The Business Area is a collection of single or multiple Business Entities/ Units to which GPC expenditure is charged.
Business Area Authority	Individuals within the Business Area that has the appropriate level of authority to sign off spend within their BE/BU (e.g. Budget Holder/Finance Director/Head of Unit/Finance Manager).
Business Entity/ Business Unit	This is a unique Cost Centre to which GPC expenditure will be charged. Through the course of this document this will be referred to as BE/BU.
Delegated Financial Authority/ Statement of Financial Authority	For **NOMS**, financial authority to purchase is delegated to Cardholders via form PHX040, authorised by the Budget Holder. For **MoJ**, a formal letter issued to cardholders stipulating allowable purchases on behalf of the Department and credit limits. Throughout the course of this document both of these items will be referred to as Delegated Financial Authority.
Liberata	MoJ outsourced finance services.
Smartdata	Smartdata is an online management tool which provides the Business Area, Card Administrators and Card Holders with the ability to review card transactions online within 24 hours of the transaction being posted to the card account.

Section 1: Policy

1. Policy introduction

1.1 Purpose of this policy document

In conjunction with the GPC Cross Government Policy this document outlines the policy and procedures governing the Government Procurement Card (GPC) scheme for purchasing across Ministry of Justice (MoJ). It outlines the roles and responsibilities of the Business Area, Card Administrators, Cardholders and the GPC Programme Administration Team. **These policies apply to ALL elements of MoJ using the GPC card.**

Note: all staff involved in the administration of the GPC or who require a GPC must read this document prior to applying for a card.

All staff must follow the policies and procedures given in this document and its associated forms.

Staff should also refer to (MoJ) Finance and Procurement policies as not all policies that govern purchasing and payment practice in general are specifically described here.

(All cross-references quoted in brackets refer to sections in this document.)

1.2 GPC Governance and Assurance

GPC Governance and Assurance is required within an overall framework of checks.

These are as follows:

- Separation of duties (there must always be a separation of duties between the Business Area Authority, Card Administrator, Deputy Card Administrator and Cardholder).
- Demonstrable audit trails.
- Meaningful and regularly produced management reports.
- Data integrity checks and compliance checks.

1.3 GPC overview

A GPC is a MasterCard branded purchasing card, operated within MoJ via J.P. Morgan. It is the preferred method of purchasing and payment for low value goods or services.

The GPC is not intended to replace the current purchasing and payment systems, but to complement MoJ purchase order systems in accordance with the Procurement Acquisition Model.

GPC Cardholders must only use the card for official business purposes. Misuse of the GPC card may result in disciplinary action and/or criminal proceedings.

Where queries are raised with Card Administrators regarding Cardholder transactions it may be necessary on occasion for the GPC Programme Administration Team to report their responses to senior officials and MoJ Head of Audit. Failure for Card Administrators to respond to queries could result in the cancellation of cards.

1.4 GPC Transparency

In accordance with the requirements of the Cabinet Office Transparency Board, MoJ must publish GPC transactional level data of £500 and over on the MoJ internet. This data is published monthly in arrears.

Publishing data will provide:

- Visibility to the use of the GPC card to the general public
- Evidence of control and compliance.

Before publication the data will be distributed to the relevant Operating Units Finance Director to arrange for the transactions to be checked, and if necessary, explained. It is important to note that the details of all transactions of £500 and over will be in the public domain.

Transactions which are seemingly not in the interest of the tax payer or do not represent general business activity may result in press and/or public interest. It is the responsibility of Cardholders, Card Administrators and their Business Area to be able to justify any transaction they make which places them on or above the £500 threshold.

2. Policy regulations and restrictions

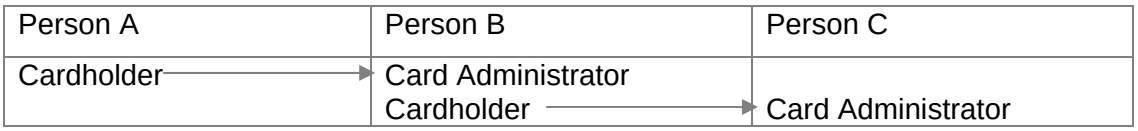
2.1 Administration and authorisation

All staff must ensure compliance with all business rules and purchasing restrictions.

- All staff that are given responsibility for GPC authorisation, administration and usage must be permanent members of staff.
- Business Areas can have more than one Cardholder and more than one Card Administrator. It is recommended, if possible, that the Card Administrator is the line manager or a more senior member of staff.
- Each Card Administrator can check the purchases of more than one Cardholder as long as the Cardholder is assigned to them.
- Only requests from nominated Card Administrators for changes to Cardholder details or to set up new Cardholders will be actioned by the GPC Programme Administration Team.
- To ensure the risk of fraud and misuse is mitigated Card Administrators in general must not hold a card themselves. It is accepted that on occasion this situation may be unavoidable, particularly in smaller offices. Should this situation arise then the Card Administrator must be authorised by the Business Area Authority to become a Cardholder, and as such must report to a separate Card Administrator. That is to say:

Prohibited

Allowed



2.2 Delegated Financial Authority

It is the responsibility of the budget holder to ensure Cardholders have the correct delegated authority.

Delegated Financial Authority

- Cardholders must always have the authorised level of Delegated Financial Authority obtained from their Business Area before making purchases.

GPC Delegated Authority

- Cardholders must always have authorised level of GPC Delegated Authority obtained from their Business Area before making purchases.

  Note to MoJ Staff **Only**: Your GPC Delegated Authority will form part of your Statement of Financial Authority.

Currently each card can only be associated with one Business Entity/Unit (BE/BU). However, should there be a requirement to purchase on behalf of more than one BE/BU then the GPC Programme Administration Team (PA) should be contacted in order to make arrangements with the bank to set up the necessary hierarchy against the relevant Cardholder's card. Cardholders should not apply for a second card.

2.3 GPC credit limits

Each card carries two limits for control purposes, these are:

- 'Single transaction limit', this is the maximum value that can be purchased for each individual transaction.
- 'Monthly credit limit', this is the total amount that can be purchased within each monthly cycle. (The cycle runs from the 29th of one month to the 28th of the next, inclusively.)

All new cards are set as standard with a £1,000 (inclusive of VAT) single transaction limit and a £5,000 (inclusive of VAT) monthly limit; Card Administrators have no authority to amend this amount.

Any requests for change need to be referred to the Business Area Authority on a case by case basis with full business justification. Request should be made through the *Change of information form* and forward to the Business Area for authorisation before submission to the GPC Programme Administration Team.

2.4 GPC application forms and personal data

Card Administrators must ensure that the applications forms are completed in accordance with the GPC policy administration.

Acceptance of the *Personal data form* terms and conditions are a mandatory legal requirement under Financial Services Authority (FSA) rules and must be signed by each GPC Cardholder.

The *Personal data form* must then be returned to the Card Administrator to keep on record as evidence of acceptance.

2.5 GPC purchasing rules

The following rules apply for Cardholders making purchases with their GPC:

- For each requisition, the Cardholder should first follow all necessary procedures to ensure value for money before making the purchase.
- MoJ contracted suppliers must be used whenever possible to ensure value for money and increased security of GPC details.
- The Cardholder must always personally place the order.
- Cardholders must never arrange with suppliers to split a single purchase over more than one payment in order to avoid exceeding their single transaction limit.

  Note: compliance with this rule is being monitored and repeated non-compliance will result in being reported to MoJ Head of Audit and cancellation of the GPC card.
- When using a GPC, Cardholders must never personally benefit by gaining points on store loyalty cards, accepting sales vouchers or by any other means. This breaches policy on propriety and will be treated as a disciplinary offence.
- The Cardholder must always ask for the sales receipt or goods received note to be sent with the goods when ordering over the phone.

  Note: Cardholders should also be mindful to ensure that a VAT receipt is obtained for all transactions paid for by GPC unless the supplier has payment terminals capable of transmitting electronic VAT information.

  The VAT receipt should be marked for information purposes only and not for payment. Any invoices received for GPC purchases should be returned to the supplier.
- When an incorrect amount has been charged, the Cardholder must approach the supplier to resolve the problem within 48 hours of receiving the statement.

2.6 GPC restrictions on use

The GPC card must never be used to make purchases contrary to MoJ strategies and purchasing policies. This means that the cards cannot be used to purchase goods and services from an alternative supplier where a contract exists.

Off-contract spend is monitored centrally by the Procurement Compliance Team and will be challenged.

Blocks applied to GPC Merchant Category Groups (MCG) or GPC Merchant Category Codes (MCC) apply to all cards.

In special circumstances where there are operational difficulties which cannot be avoided cards may be unblocked for an individual transaction. A business case should be sent to the Procurement Compliance Team for consideration and potential referral to the MoJ Value for Money Committee for authorisation.

2.7 Purchases prohibited by GPC policy

GPC **must not** be used for:

- obtaining cash
- paying invoices
- direct debits – acceptable in exceptional circumstances only, and with prior authorisation
- making payments that fall under the Construction Industry Scheme (CIS)
- payments to suppliers who have breached GPC terms and conditions. Cardholders will be notified of these suppliers by the GPC Programme Administration Team
- purchase of capital equipment
- purchasing items that are available from Branston Store (NOMS only)
- Oyster Cards: Exceptions will be considered on the submission of a business case for Oyster cards for groups/offices. The business case must be approved by the Operational Unit Director and then submitted to the Financial Management Committee for a decision. Where a standing process is already in place, a business case must also be submitted to ensure that the needs still comply with the current policy requirements
- payment gateways, e.g. PayPal whereby card details are stored with the gateway supplier
- spend associated to Travel and Subsistence expenses.

GPC MasterCard is categorised into 34 Categories of spend. Cardholders have access to all these groupings except those listed below.

GPC Category Description	MoJ Blocked Y/N	NOMS Blocked Y/N	Comment
Utilities and Non Automotive Fuels	Y	Y	
Telecommunications Services	Y	Y	
Catering and Catering Supplies	Y	Y	**NB: it is not permissible for staff to purchase tea/coffee or lunches for internal meetings**
Staff – Temporary Recruitment	Y	Y	
Personal Services	Y	Y	
Professional Services	Y	Y	
Financial Services	Y	Y	
Clubs/Assoc & Organisations	Y	Y	

GPC Category Description	MoJ Blocked Y/N	NOMS Blocked Y/N	Comment
Office Stationery, Equipment & Suppliers	Y	Y	**NOMS staff**: refer to Banner Catalogue on I-Procurement **MoJ staff**: refer to Banner website http://www1.banner-online.biz/
Computer Equipment & Services	Y	Y	
Miscellaneous Industrial/Commercial	Y	N	
Automotive Fuel	Y	Y	**NOMS staff**: please use fuel cards for car hire. **MoJ staff**: fuel expenses should be submitted through iExpenses or equivalent.
Travel – Air/Rail/Road	Y	Y	**NOMS and MoJ staff**: bookings **must** be made through the central travel contract with Redfern Travel Ltd. Oyster Cards if purchased for business should be reclaimed via iExpenses or equivalent.
Auto-Rental	Y	Y	**NOMS staff**: bookings must be made through Enterprise on iProcurement. **MoJ staff**: bookings must be made through the Enterprise online booking system.
Hotels & Accommodation	Y	Y	**NOMS and MoJ staff**: bookings must be made through Calder Conferences.
Restaurants & Bars	Y	Y	
Leisure Activities	Y	Y	

2.8 GPC non-compliance reports

Monthly non-compliance reports are automatically made available through Smartdata to the Procurement Compliance Team and the GPC Programme Administration Team for review. Where unauthorised purchases have been made; these will be reported to the Financial Management Committee (FMC) and the Unit Director for further investigation.

If you have questions about specific purchases please consult your Card Administrator in the first instance or the GPC Programme Administration Team.

2.9 Prisoner Goods & DHL cards (NOMS only)

Cards which are used to purchase on the behalf of Prisoners are exclusively for this purpose. Any cardholder making purchases of goods/services on behalf of the establishment on a Prisoner Goods/DHL card is in serious breach of GPC Policy. The use of Prisoner Goods/DHL cards is closely monitored by Procurement Compliance.

2.10 Contingency cards

Cards which are used to purchase in operational emergencies are exclusively for this purpose. The use of Contingency cards is closely monitored by Procurement Compliance and each contingency transaction requires Business Justification.

2.11 Delivery of goods purchased with GPC

It is GPC policy that all orders must be delivered to an official departmental address, ideally orders should be delivered to the Cardholder; however, it may be operationally necessary for orders to be delivered to a central store. Cardholders should state the delivery location when placing an order. Any *Goods received notes* sent by the supplier (including those sent to stores) should be retained with the *Purchase transaction log.*

Regulations state that the supplier must be in a position to dispatch the goods before a transaction is processed. If the supplier has to place a back order because the goods are not in stock the transaction cannot be undertaken until the goods are available for despatch. At this time the supplier should contact the Cardholder for authorisation.

Note: where the supplier agrees to credit returned goods or failed service, they must apply the credit to the GPC card that made the purchase.

3. Record management policy

3.1 Importance of record management

Record management is essential to the success of the GPC MasterCard. GPC *Card statements*, *Purchase transaction logs* and all associated documents are to be retained in hard copy to support the financial statements and reduce the risks of fraud or of staff being left in a vulnerable position should queries about individual purchase arise subsequently. This means documents for the current financial year, plus the six previous financial years. All documents should be kept in a secure location and be available for Audit as required.

4. Risk management policy

4.1 Importance of risk management

A Budget Holder/Finance Director/Head of Unit/Finance Manager must carry out spot checks on GPC transactions inline with their own local risk management checks and compliance controls. The checks must be performed by a member of staff who is neither a Card Administrator nor a Cardholder.

It is the Card Administrators responsibility to report any forms of misuse, irregularities or potential breaches of propriety to the GPC Programme administrators.

Checks must be made to ensure GPC transactions made for T&S expenses are not claimed elsewhere.

Cardholder/Card Administrator lists must be verified each month with the Business Areas. Any discrepancies noted must be reported to the GPC Programme Administration Team.

5. Card security and fraud awareness policy

5.1 Importance of card security and fraud awareness

The potential for frauds or Cardholder misuse is a key risk in the use of the card programme. A number of key controls have been built into the system to prevent, detect and deal with this.

The transaction and monthly spend limits are outlined in Section 1: Policy (2.3). CHIP & PIN provides added protection for point of sale transactions and the ease with which transactions can be traced is also a deterrent.

All staff (where applicable) must forward the details of all known incidents of fraud or suspected fraud to MoJ Head of Audit.

If you suspect any fraud on your card the Cardholder must notify J.P. Morgan immediately using the 24-hour customer service. The bank will cancel the card and arrange to issue a replacement. Ensure that you have details of the suspected transaction when making the call.

Where fraudulent activity has been suspected, the Card Administrator should cut the card through the magnetic strip and the chip and dispose of it in confidential waste.

All users have a responsibility to make themselves aware of the areas of risk, and of what to do if fraud is suspected. What follows are the key points with regard to GPC.

5.2 Receiving your card and PIN

Cards are provided to named Cardholders and are not transferable.

Upon receipt the Cardholder must memorise and destroy the PIN in confidential waste.

5.3 Securing your card

When the GPC card is in use the Cardholder should retain the card on their person at all times, and never leave it unattended.

When the GPC card is not in use, it must be locked in a secure place and should only be accessed by the Cardholder.

5.4 Non disclosure of card details and PIN

The GPC card should never be photocopied.

When making a purchase in person, the Cardholder should never let a cashier take the GPC card away, out of sight. If this happens the Cardholder must report the incident as suspected fraud.

The Cardholder should not disclose the full 16-digit number of the card to any other member of staff, with the exception of their Card Administrator or Business Area Authority. Some GPC forms require the full card number. These forms should only be completed by Cardholder and Card Administrator/Business Area Authority and only sent to the GPC Programme Administration Team.

Never email or fax any card details to suppliers.

Cardholders are expected to take reasonable care to avoid inadvertent disclosure of their card number, and to be aware of their surroundings and those present when using the GPC card. In particular, they should take care when using the card in public areas or over the telephone.

The Cardholder should never disclose their PIN or three-digit security code to any other staff member in any situation. If this happens accidentally (or the Cardholder suspects it has happened), Cardholders should contact the GPC Programme Administrators to request a new PIN, or GPC card. Never write the PIN or security code down.

5.5 GPC online card security

When purchasing online, Cardholders should always ensure they are using a secure site. The Internet address for secure sites begins ‘https’ and not just ‘http’. Please refer to current best practice guide for purchasing over the internet available on the GPC intranet page.

The Cardholder must never reply to emails purporting to be from the bank. All genuine communication regarding GPC will be sent from the GPC Programme Team.

Section 2: Roles and responsibilities

This section briefly defines the roles and responsibilities that individuals have when managing and utilising the GPC on behalf of Ministry of Justice.

1. The Business Area Authority

1.1 Business Area Authority role

The Business Area Authority is defined as an individual that has overall personal responsibility for the governance and compliance of the GPC within their Business Area. Commonly this role would be fulfilled by a Director, Senior Manager, Budget Holder, Head of Unit or Finance Manager.

Note: agency and interim members of staff are not eligible to manage or hold a GPC Card

1.2 Business Area Authority responsibilities

The Business Area Authority is responsible for the following:

- justifying the requirement for a GPC within their Business Area
- appointing a deputy to the Business Area who will manage the roles and responsibilities in the absence of the Business Area Authority
- nominating Cardholders, Card Administrators and Deputy Card Administrators for the Business Areas respective Business Entity/Business Unit(s)
- delegating financial authority to Cardholder(s) in accordance with Ministry of Justice Finance policy and process
- ensuring that GPC is properly utilised by all its Cardholders
- ensuring that Prisoner Goods/DHL cards are used solely for purchasing on behalf of Prisoners using Prisoner Monies.
- all purchases made by GPC by the nominated Cardholders
- setting GPC credit limits
- amending GPC credit limits

  Note: amending credit limits is time consuming. Careful planning should help to avoid having to do this unnecessarily. Card limits will not be increased unless sufficient justification is provided by the cardholder and approved by the Business Area Authority.
- performance of all local risk management checks and compliance controls
- initiating disciplinary action when the GPC is misuse.
- validation of GPC transaction data in readiness for transparency publication on MoJ website

2. The Card Administrator

2.1 Card Administrator role

The Card Administrator is a permanent member of staff nominated by the Business Area to manage the day to day administration of the GPC card for the business entity/unit.

2.2 Card Administrator responsibilities

The Card Administrator is responsible for the following:

- appointing with their Business Area Authority a suitable deputy (Deputy Card Administrator) to manage these roles and responsibilities during any period of absence
- assisting the card requester with the application process. Card Administrators must check and ensure that the card requester has read the GPC policy and is aware of their obligations before using the card
- ensuring that the card requester has read and understood the personal data terms and conditions contained within the electronic application form and that they have signed a hard copy of which the card administrator must secure locally
- validating the data within all card applications before forwarding to the GPC Programme Administration Team for processing
- ensuring that GPC cards and PINS are distributed to Cardholders as appropriate and *Card and PIN acknowledgement forms* are completed and retained locally for audit purposes
- maintaining a list of cardholders and their business contact details for communication and administration purposes
- checking their Cardholder(s) purchases and documentation each month, reconciling the *Purchase transaction log* with the *Card statement* and recording any errors, mismatches, omissions or potential misuse
- arranging for *Card statements*, *Purchase transaction logs* and all associated documents to be retained for the current financial year plus the previous six years as per audit requirements
- Resetting of their Cardholder's passwords and reactivation of Card accounts in Smartdata.
- reporting any misuse or non compliance to the GPC Programme Administration Team
- updating the GPC Programme Administration Team with any changes in their details or those of their Cardholder via the *Change of information form*
- ensuring card security during any long term absence of the Cardholder
- appropriate disposal of old or expired cards
- production of management information reports via Smartdata as and when requested by the Business Area.

3. The Deputy Card Administrator

3.1 Deputy Card Administrator role

The Deputy Card Administrator is a permanent member of staff nominated by the Card Administrator and the Business Area Authority to manage the day to day administration of the GPC card for the Business Entity/Unit.

3.2 Deputy Card Administrator responsibilities

The Deputy Card Administrator is responsible for the Card Administrators responsibilities in any period of the Card Administrator's absence.

4. The Cardholder

4.1 Cardholder role

The Cardholder is a permanent member of staff nominated by the Card Administrator who has been assigned the appropriate level of delegated financial authority by the Business Area to purchase goods and services via GPC in accordance with the MoJ procurement acquisition model and the GPC policy for their Business Entity/Unit.

4.2 Cardholder responsibilities

The Cardholder is responsible for the following:

- compliant use of the GPC card as outlined in the GPC policy
- must ensure that all necessary procedures to ensure value for money are followed for each requisition
- is responsible for the security of their assigned card, card number and PIN [Section 1:Policy (5)]
- keep an accurate and up-to-date *Purchase transaction log* [Section 3: GPC Administration (4.1)]
- must access and download the monthly *Card statement* from the bank through Smartdata [Section 3:GPC Administration (5.2)]
- must reconcile their *Card statement* with their *Purchase transaction log*, confirming that the details accurately reflect the purchases made, and submit the *Purchase transaction log* along with all other documents to their Card Administrator at the end of each month for approval
- must ensure that any overcharges are credited back to the GPC card
- must retain GPC spend receipts and associated documents
- must raise any GPC queries with the GPC Programme Administration Team
- must update GPC Programme Administration Team of any changes (e.g. maternity leave).

Note: Cardholders are reminded of the need for care when using the card and particularly in the selection of suppliers used to make purchases. Where possible, a contracted supplier should always be used as prices charged will have been determined in advance.

5 The Regional/Group/ Directorate Finance Office (HMCS and Tribunals only)

5.1 HMCS & Tribunals Group role

This role is also known as the Regional Card Administrator (RCA) The RCA is a permanent member of staff.

5.2 HMCS & Tribunals Group responsibilities

The RCA is responsible for the following:

- monitoring compliance, regularity and propriety and for managing controls
- performing a spot check on 10% of all GPC transactions made within its Business Area
- verifying Cardholder/Card Administrator lists each month with the Business Area Authority. Any discrepancies noted must be reported to the GPC Programme Administration Team.

6 The GPC Programme Administration Team

6.1 GPC Programme Administration Team roles

The GPC Programme Administration Team are the first point of contact for Card Administrators and Cardholders in relation to GPC general programme administration and control.

6.2 GPC Programme Administration Team responsibilities

The GPC Programme Administration Team is responsible for the following:

- providing the Business Areas with assurance within an overall framework of compliance checks via analysis of GPC transactional data.
- issuing key communications to GPC users
- processing card applications and validating card accounts
- dealing with any GPC cardholder account queries, e.g. unblocking cards, amending card limits
- are the first point of contact with the bank (J.P. Morgan)
- arranging for all payments to be made through the agreed finance process
- providing Liberata with card data to enable correct recharging to the BE/BUs
- day-to-day maintenance of Smartdata information for Cardholders, Card Administrators, and Business Area Authorities responsible for GPC via the *Change of Information form*
- to provide ad hoc/monthly management information upon receipt of an *Application for management information* where staff do not have access to Smartdata.

Section 3: GPC administration

1. Account opening mandate

1.1 Business Area account opening mandate

Each Business Area is required to set up an account with J.P. Morgan and it is mandatory that an *Account opening mandate form* is completed before any application forms can be processed by the Business Area Authority.

Copies of the *Account opening mandate form* are available from the GPC Intranet page and must be returned to the GPC Programme Administration Team via email.

1.2 Nominating the Card Administrator and the Cardholder

When the Business Area has set up an account it must nominate a suitable Card Administrator, Deputy Card Administrator and Cardholders, who must have written delegated financial authority from the budget holder. A description of these roles is given in Section 2: Roles and Responsibilities (2, 3, and 4). The nominees must be provided with a copy of this policy and asked to read it through. They must be able to demonstrate an understanding of their responsibilities.

2. Card application, distribution and activation

2.1 Card application process

To apply for a J.P. Morgan GPC, a *Cardholder application form* must be completed by each requestor and emailed to the BE/BU assigned Card Administrator. Guidance on how to complete the *GPC application form* is available via the MoJ intranet GPC webpage.

The Card Administrator must approve the Cardholder's *GPC application form* and validate its contents including the BE/BU reference numbers and retain locally the card requestors' signed *Personal data form* [Section 1: Policy (2.4)].

The authorised GPC application form and *Account opening mandate form* must then be sent by the Card Administrator to the GPC Programme Administration Teams' functional mailbox and copied to the Business Area Authority to confirm approval.

Forms will be checked and verified by the GPC Programme Administration Team.

Incomplete applications will be rejected back to the Card Administrator. Please note personal postal and/or email addresses will not be accepted. Phone numbers must be work landline numbers only.

Approved applications will then be forwarded to J.P. Morgan within two working days.

2.2 Card distribution

All new cards and PINS will be sent to the Card Administrator's business address. Cardholders will need to arrange to collect cards from their Card Administrator. Business as usual will see cards delivered within 5–7 business days.

When Cardholders collect their new card, they must complete an *Acknowledgement of card and PIN receipt form*.

At this time the Cardholder must handover their existing cards to the Card Administrator, who will arrange to destroy the card securely.

The PIN will be sent separately from the GPC card and once received the Cardholder must memorise and destroy the PIN in confidential waste.

Card Administrators will need to contact the GPC Programme Administrators if the card or PIN is not received within ten working days.

If Cardholders lose their GPC or forget their PIN, they should contact the GPC Programme Administrators to request a new PIN, or GPC card. Never write the PIN or security code down. To report lost or stolen cards [Section 3: GPC Administration (8.1)].

2.3 Card activation

Upon receipt of the new GPC card, instructions will be included regarding the activation process.

3. Purchasing process

3.1 Purchasing methods

Purchases can be made in one of the following ways:

- by telephone and quoting the card number
- by using the internet, via a secure site, providing the necessary card and delivery details (for further details see Purchasing over the internet – Annex A)
- by visiting the supplier's premises and using CHIP & PIN/signing for the goods.

For security, a supplier may request the billing address of a card. For all cards, this is the Cardholder's business address.

Cardholders must not issue purchase orders where GPC has been used.

3.2 Items received into NOMS/HMPS Stores

Cardholders have ultimate responsibility for ensuring that the *Purchase transaction logs* are completed according to policy.

For items received into stores, the Store manager is responsible for updating the *Purchase transaction log* when the goods are received. To facilitate this process it is important that stores are given access to *Purchase transaction log(s)* available from the GPC website. Items that have been part delivered should be

recorded as such to notify the Cardholder to ensure they take this into account when reconciling statements.

Where goods are received directly by the Cardholder the original requisitioner must make an entry on the *Purchase transaction log* as independent verification that delivery has occurred.

4. The *Purchase transaction log*

4.1 *Purchasing transaction log* recording and reconciliation

A *Purchase transaction log* is a record of all purchases made using the GPC card. An electronic version of the *Purchase transaction log* is available from the GPC intranet page. When completing the *Purchase transaction log* ensure the following:

- Each purchase must be recorded on the log as it is made.
- Each transaction must be given a unique identifying reference on the log, which should be copied onto each matching receipt. Best practise holds that the *Purchase transaction log* should be updated at the point the goods or services are purchased.
- All receipts and delivery notes should be kept with the *Purchase transaction log*. If your purchase is over the phone, then remember to ask your supplier to ensure that the sales receipt/goods received note is sent to you when the goods/services have been delivered.

Transactions made just prior to the end of the monthly card cycle (28th of each month) may not appear on the card statement until the following month. The Card Administrator should mark these as carried forward on the *Purchase transaction log*, and ensure that the Cardholder carries them forward to their next months' *Purchase transaction log*.

At the end of each month, the Cardholder must sign the *Purchase transaction log* to confirm that all purchases were made for business purposes only. Upon receipt and reconciliation of the card statement and *Purchase transaction log*, the Cardholder must send either a nil return, or the *Purchase transaction log*, along with supporting documentation to their Card Administrator.

The local transaction reference, given by the Cardholder, should be written against the corresponding transactions on the card statement so that a clear audit trail is maintained.

The Card Administrator must also confirm that the:

- purchases were appropriate and made for the Department
- goods or services were received
- price was fair and reasonable.

They must sign the card statement and retain all documentation.

5. Cardholder statements

5.1 What is Smartdata?

Smartdata is a J.P. Morgan internet-based reporting and expense management solution which provides the Business Area Authority, Card Administrators and Cardholders with the ability to review card transactions online within 24 hours of the transaction being posted to the card account in the system.

In accordance with the sustainability agenda, hardcopy *Cardholder statements* will no longer be provided. All *Cardholder statements* will be available electronically through J.P. Morgan's online management tool, Smartdata.

5.2 Cardholders access to Smartdata

Access to the system will be made available to GPC Cardholders to be able to view their transactions and monthly statement online. Login details are provided via the *Quick reference Cardholder guides* available from the GPC intranet page.

Cardholders will be able to access their monthly card statement online through Smartdata, **one day** after the monthly cycle ends.

If the Cardholder has made transactions within the monthly cycle, but is unable to access their *Card statement* online, they should inform the GPC Programme Administration Team as soon as possible.

A *Card statement* will not be system generated if no transactions have been made in the monthly cycle. In this case the Cardholder must send a signed 'Nil Return' *Purchase transaction log* to their Card Administrator.

Where transactions have been made, the online GPC *Card statement*, *Purchase transaction log* and all supporting documents must be sent to the Card Administrator within **five days** of receipt of the online card statement.

5.3 Card Administrator access to Smartdata

Access to the system will be made available to Card Administrators via the *Account opening mandate*. J.P. Morgan will email Card Administrators with their log-in details accordingly.

To enable Card Administrators to view and report on Cardholder transactions and spend data within their BE/BU, *Quick reference Card Administrator guides* will be provided as separate documentation available from the GPC intranet page.

5.4 Disputed transactions and unsatisfactory goods and services

Cardholders may from time to time want to query a transaction on their statement. This can be for a number of reasons such as:

- the card statement lists an item that the Cardholder does not recognise, and cannot be reconciled with their *Purchase transaction log*
- the incorrect amount has been charged [Section 3: GPC Administration (5.5 below)]
- refunds not applied to the GPC card

- faulty or damaged goods supplied, refund requested
- goods/services not supplied
- wrong goods/services supplied.

J.P. Morgan may need the Cardholder to complete a *Declaration form* or supply copies of correspondence with the supplier. Once they have receipt of this, the bank will perform a thorough investigation with the merchant(s) in question, and will endeavour to get the disputed amount credited back to the Cardholder's GPC account.

Note: J.P. Morgan only have limited time span to query transactions with the supplier. Therefore it is important that the Cardholder advises J.P. Morgan of any queries within 30 days from the statement date.

5.5 Incorrect amount charged to card

When an incorrect amount has been charged, the Cardholder must first approach the supplier to resolve the problem within 48 hours of the statement being made available in *Smartdata.*

If the supplier insists on the transaction being genuine the Card Administrator must raise the issue with J.P. Morgan. If no explanation follows, the transaction should be treated as a disputed item [See 3 (5)].

5.6 Goods charged but not received

If the Cardholder is charged for items that have not been received (goods/services), they should firstly contact the supplier to ensure that the goods have been delivered to the correct address. (It is a regulation set down by MasterCard that the transaction is not processed until the goods are allocated for dispatch.)

If the supplier insists that the goods have been delivered, treat the transaction as a disputed item.

The majority of the time these issues can be resolved by the Cardholder contacting the supplier directly. If the Cardholder is unable to resolve with the supplier they should contact **J.P. Morgan Customer Services**.

5.7 Unsatisfactory goods or services

The Cardholder must raise any disputes relating to unsatisfactory goods immediately with the supplier. If they cannot come to a mutual agreement with the supplier, they should contact the GPC Programme Administration Team as soon as possible.

Any credit amount agreed with the supplier must be recorded on the *Purchase transaction log*.

Note: contact the GPC Programme Administration Team immediately if a supplier insists on sending a cheque instead of applying credit to the GPC for returned goods or failed service.

6. Change of information

6.1 Changing Cardholder details, credit limits and cancelled cards

Card Administrators should ensure that the GPC Programme Administration Team is notified of any change in their contact details, or those of their Cardholder(s) through the *Change of information form*. Failure to do so increases the risk of fraudulent transactions being made on the GPC cards and BE/BUs will be liable for any loss incurred in this instance.

6.2 Change of Cardholder's name

If a Cardholder changes their name, a *Change of Information Form* should be completed and emailed to the GPC Programme Administration Team. A new GPC card, with the same 16 digit card number, will be issued within **ten** working days.

6.3 Changing Business Areas

The Business Area Authority can change a card's BE/BU allocation, using a *Change of information form*, which must be completed and emailed to the GPC Programme Administration Team. The Cardholder must have the appropriate delegated financial authority for the new BE/BU.

If the cardholder is moving to a new Business Area then the *Change of information form* must be authorised by the authority within that Business Area. This also includes existing Cardholder's moving from one BE/BU to another.

6.4 Amending credit limits

The Business Area Authority can adjust credit limits, but must assess its requirements for each card carefully in order to set the limits at an appropriate level. The limits should be high enough to enable the Cardholder to make the purchases expected of them, whilst low enough to act as a control. To apply for a change to credit limits a *Change of information form* must be completed by the Card Administrator and approved by the Business Area Authority.

Amending credit limits is time consuming. Careful planning should help to avoid having to do this unnecessarily.

6.5 Cancelling cards

The Card Administrator must email a completed and approved *Change of information form* as soon as possible to the GPC Programme Administration Team. If the Cardholder is leaving the department, this form must be completed beforehand; so that a specific date can be given.

To destroy the card, the Card Administrator must cut through the magnetic strip of the card and the part of the card containing the chip and dispose of it in confidential waste.

6.6 Long-term absence

If a Cardholder is on long-term absence, it is the Card Administrator's responsibility to ensure the security of the card. They must:

- lock the card in a secure cabinet
- send a *Change of information form* to the GPC Programme Administration Team, requesting that the monthly transaction limit of the card is set to zero.

When the Cardholder returns to work, the card should be returned and a request made via the *Change of information form* for the credit limit to be reset.

If the card remains inactive for a period of six months (and the GPC Programme Administrators have not been advised of a long-term absence, [as per Section 3: GPC Administration (6.6)] the card is subject to cancellation

6.7 Withdrawn cards

Card Administrators must ensure the destruction of cards that are withdrawn or no longer required for any reason and to notify the GPC Programme Administration Team in order for them to cancel the card.

7. Reporting and management controls

7.1 Reports for Regional/Group/Directorate Finance Offices

Monthly transaction reports and Cardholder/Card Administrator reports will be provided by the GPC Programme Administrators on application for this purpose (use a *Management information application form*).

Access to Smartdata may be given for regular reports to be run locally following justification, security and audit review. Specific requests can be made via the GPC Programme Administration Team.

7.2 Business Area management controls

The Business Area must carry out its own local risk management checks and compliance controls. They must ensure:

- checking and endorsement of original documentation – *Purchase transaction log*, *Card statement*, receipts and delivery notes – recording any errors, omissions or non-compliance [Section 1: Policy (3 & 4)].
- logging of all Cardholders within the BE/BU and their credit limits, to act as the basis for random checks on the physical presence of the GPC cards and for risk assessment purposes. **Note: card numbers should not be recorded on this log.**

7.3 GPC Transparency Reporting

Prior to the mandatory publication of GPC data and at the end of the GPC statement period the Procurement Compliance Team will distribute to each Business Area Authority (Finance Director or equivalent) GPC transaction data for spend £500 and over, relevant to their area of responsibility.

Individual transactions must be verified, and where necessary, redacted in accordance with FOI guidelines. Press lines must also be provided to explain any transactions that may be likely to attract press attention. Business Areas will also be required to respond to any queries following publication of the transaction data.

Upon completion of the above, confirmation of data for publication must be sent to the Procurement Compliance Team within the defined deadlines.

8. What to do if a card is lost or stolen, or declined

8.1 What to do if a card is lost or stolen

If your card has been lost or stolen, the Cardholder must notify J.P. Morgan immediately using the 24-hour customer service line.

J.P. Morgan will cancel the card, ensuring that no further transactions can be made. They will then make the necessary arrangements for a new card to be issued to the Cardholder via the Card Administrator. The Cardholder should ensure they confirm their Card Administrators current business address ensuring the GPC card is delivered to the correct location.

Note: the bank will cancel the card and arrange to issue a replacement, with a different 16-digit number. The Cardholder must complete a *Change of information form* and email it to the GPC Programme Administration Team.

All new cards and PINS will be sent to the Card Administrator's business address. Cardholders will need to arrange to collect cards from their Card Administrator.

When Cardholders collect their new card, they must complete an *Acknowledgement of card and PIN receipt form* [Section 3: GPC Administration (2.2)].

8.2 What to do if a card gets damaged

Cardholders should inform the GPC Programme Administration Team if their card gets damaged. The Card Administrator should forward the Cardholder's name and last 10 digits of their card to the GPC Programme Administration Team, who will be able to order a replacement.

The new card will have the same 16-digit number.

The Cardholder should cut the card through the magnetic stripe and the part of the card containing the chip and dispose of it in confidential waste.

8.3 What to do if a GPC card is declined?

If a GPC card or transaction is declined Cardholders must:

- first check with the supplier that all the details they have are correct
- ensure they have sufficient credit on their GPC card; if not, seek authority from their Business Area Authority to initiate an amendment [Section 1: Policy (2.3)]
- check they are not making purchases listed in the *GPC Prohibited purchases list* [Section 1: Policy (2.7)].

If the Cardholder has sufficient credit, and is sure the supplier has all correct details, they need to refer the problem to the GPC Programme Administration Team. Their Card Administrator also should be made aware of the issue.

9. GPC forms and service levels

9.1 Table of forms

This table lists all GPC forms, how they should be sent, and the process turn around times.

Form	To be held by…	Method of delivery	GPC Programme Administration Team (PAT)	J.P. Morgan Customer Service Team
Financial authority	Cardholder & cc'd to Card Administrator	N/A	N/A	N/A
Account opening mandate	PAT	Email	Up to two working days	Up to ten working days
GPC application form	PAT	Email	Up to two working days	Up to ten working days
Data security form	Cardholder & cc'd to Card Administrator	N/A	N/A	N/A
Acknowledgement of card and PIN receipt form	Card Administrator	N/A	N/A	N/A
Change of information form	PAT	Email	Up to two working days	Up to ten working days
Management information form	PAT	Email	Reports will be provided at the end of full calendar month	N/A

All forms are available from the GPC MoJ intranet pages

Produced by Ministry of Justice