EFFECTIVE FROM February 2020

Data Protection Policy

1. Definitions

DPO	Data Protection Officer.
GDPR	Means the General Data Protection Regulation (EU) 2016/679 on the protection of all individuals within the European Union (EU) and the European Economic Area (EEA) with regard to the processing of Personal Data and on the free movement of such data.
Data Subject	Means a living individual that can be identified directly or indirectly from the Personal Data we hold. All data subjects have legal rights in relation to their personal information.
Data Protection Impact Assessments	Means a data protection impact assessment, being an assessment of any privacy risks associated to any processing of Personal Data by MOPAC and any processes and controls in place to mitigate or eliminate such risks
Personal Data	Information relating to an identified or identifiable individual.
Process or Processing	Any operation or set of operations which is performed on Personal Data, including collecting, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing, disseminating, combining, restricting, erasing and destroying.
Special Category Data	Information about an identifiable individual relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data

	used to uniquely identify a person, health data or data relating to sex life or sexual orientation.
Supervisory Authority	The data protection regulatory authority in the UK or a European Union Member State
Third Party	Means any person other than the Data Subject, or MOPAC.

2. Introduction

This Data Protection Policy (**Policy**) explains The Mayor's Office for Policing and Crime (**MOPAC**) policy for processing all Personal Data under the GDPR. This Policy applies to all our employees, temporary and agency workers, contractors, interns, volunteers, apprentices and contractors (referred to collectively in this Policy as **employees** or **you**).

This policy is designed to help you have all the important guidance and information you need to ensure that you can support us to meet our legal requirements, to make sure privacy is at the forefront of our minds and individuals' data is protected. When processing Personal Data, everyone at MOPAC must adhere to and respect the key data protection principles derived from the GDPR.

This policy provides information and guidelines for MOPAC when handling of Personal Data. It sets out the requirements of Data Protection Law, what MOPAC must do to comply, and the controls MOPAC has put in place to ensure compliance. If you have any questions about this Policy, please raise them with James Bottomley (DPO).

3. The data protection principles and what they mean

What is data protection? In simple terms it is the protection of information about living people. It concerns the safeguarding of privacy rights when Personal Data is processed. The GDPR sets out key principles that should be followed when you process Personal Data to ensure compliance.

Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner.

What must MOPAC do to comply?

- Under the GDPR, it is illegal to process Personal Data unless one of the legal conditions set out in the GDPR applies. MOPAC must always identify a legal basis which permits data processing.

- MOPAC must always balance the interests of MOPAC in using Personal Data against the privacy rights and expectations of the Data Subjects to ensure that use of Personal Data is fair.
- MOPAC must ensure that Data Subjects are provided with an easy to understand and easy to access explanation of how MOPAC will use their Personal Data at the point where Personal Data is collected.

How does MOPAC ensure compliance?

- When commencing new projects, MOPAC carries out Data Protection Impact Assessments (**DPIAs**) to ensure that its use of Personal Data is necessary and proportionate. See MOPAC's DPIA Policy for more information about DPIAs.
- MOPAC provides privacy notices to Data Subjects at the point of data collection, [including on its website and privacy notices are provided to internal employees/contractors as part of their induction pack.

Purpose limitation

Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

What must MOPAC do to comply?

- MOPAC must ensure that Personal Data is only used in accordance with the purposes that have been notified to Data Subjects at the point of data collection.
- If any new use of Personal Data is proposed, MOPAC must carry out an assessment to ensure that the new use is compatible with the original notified purposes.

How does MOPAC ensure compliance?

- DARA carries out regular audits of its data processing activities to ensure that processing continues to be consistent with the purposes notified to individuals, and MOPAC regularly reviews the outcomes these audits.
- When commencing new projects, MOPAC carries out Data Protection Impact Assessments (DPIAs) to ensure that its use of Personal Data is compatible with the original purpose.

Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.

What must MOPAC do to comply?

- MOPAC must ensure that it only collects and uses the minimum amount of Personal Data that is needed to achieve the purpose of processing.
- MOPAC must ensure that when sharing Personal Data with Third Parties, only the minimum necessary information is shared.

How does MOPAC ensure compliance?

- All employees are responsible for reviewing data collection points on a regular basis to ensure that only the minimum required amount of Personal Data is collected.
- When sharing Personal Data, all employees are responsible for ensuring that only the minimum amount of Personal Data is shared.

Accuracy

Personal Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified without undue delay.

What must MOPAC do to comply?

- MOPAC must put in place appropriate measures to check data accuracy by giving Data Subjects an opportunity to review and update their Personal Data at regular intervals.
- Where possible MOPAC should put in place appropriate tools to ensure accurate data is collected.
- If MOPAC is notified about inaccurate data, MOPAC must ensure that their records are updated promptly.

How does MOPAC ensure compliance?

- All employees at MOPAC are responsible for ensuring that, where necessary, they follow procedures in place for updating inaccurate records.

Storage limitation

Personal Data must be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed.

What must MOPAC do to comply?

- MOPAC must set retention periods for Personal Data and ensure that Personal Data is either anonymised, securely destroyed or erased at the end of applicable retention periods.

How does MOPAC ensure compliance?

- MOPAC has a retention policy which specifies retention periods for all Personal Data Processed. See MOPAC's Data Retention Policy for more information.
- All employees are responsible for ensuring its compliance with MOPAC's Data Retention Policy.

Integrity and confidentiality

Personal Data must be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

What must MOPAC do to comply?

- MOPAC must put in place appropriate information security measures to protect Personal Data from unauthorised access, use, loss or disclosure.

How does MOPAC ensure compliance?

- MOPAC has in place an information security policy which sets minimum standards for information security matters.
- Annual training on information security matters is mandatory for all employees.
- MOPAC reviews its continuing compliance with the information security policy on an ongoing basis, and DARA (MOPACs audit function) regularly audit MOPAC on information governance and security.

Accountability

MOPAC is responsible for, and must be able to demonstrate compliance with, the GDPR.

What must MOPAC do to comply?

- MOPAC must ensure that appropriate policies and processes are in place to enable compliance with the data protection.
- MOPAC must monitor compliance with policies and processes and take action to ensure that any issues of non-compliance are remedied by the provision of further training or other measures.
- MOPAC must regularly review the adequacy of policies and processes to ensure they enable compliance with the data protection principles.

How does MOPAC ensure compliance?

- MOPAC has a number of policies and procedures in place, as set out in [16] of this policy

- MOPAC reviews its compliance with the policies on a regular basis, and DARA (MOPACs audit function) regularly audit MOPAC on information governance and security.
- All employees must read and understand all policies and procedures and put them into practice.
- MOPAC will review all policies annually and inform employees of any changes
- MOPAC has appointed a Data Protection Officer (**DPO**) to ensure compliance with data protection laws. Your DPO is James Bottomley.

4. Rights of Data Subjects

Data protection laws also give rights to Data Subjects. These rights are set out below:

Right to be informed about how their Personal Data is used

Data Subjects have a right to be informed about how MOPAC will use and share their Personal Data. This explanation must be provided in a concise, transparent, and accessible format. Privacy notices must be written in clear and plain language and must be provided free of charge.

When the Personal data is collected directly from the Data Subject, MOPAC must ensure that it provides a privacy notices at the point of collection. If MOPAC does not collect the Personal Data directly from the Data Subject then the information must be provided to them within one month, or if earlier, at the point of first contact with the Data Subject or before their Personal Data is disclosed to a Third Party.

The GDPR sets out a list of specified information that must be provided to Data Subjects in privacy notices. MOPAC must therefore ensure that all privacy notices contain this mandatory information.

Right to access Personal Data

Under the right of access, Data Subjects have a right to:

- obtain confirmation of whether MOPAC is processing their Personal Data;
- access to their Personal Data; and
- information regarding how their Personal Data is being used by MOPAC, including if you are sharing it with Third Parties.

The purpose of the right of access is to allow Data Subjects to access their Personal Data so they are aware of and can verify the lawfulness of the processing carried out by MOPAC.

When an access request is received MOPAC must provide a copy of all Personal Data to the Data Subject unless an exemption applies.

Right to have inaccurate Personal Data rectified

Data Subjects have a right to have any inaccurate or incomplete Personal Data about them rectified.

If MOPAC has disclosed the relevant Personal Data to any Third Parties, MOPAC is also responsible for taking reasonable steps to inform those Third Parties of the rectification where possible.

If MOPAC disputes that the Personal Data is inaccurate then it will be necessary to go back to the Data Subject and explain why the information is not being rectified. Data Subjects should also be informed at this point that they have a right to complain to the relevant Supervisory Authority (**SA**) if they do not agree with this decision.

Right to have Personal Data erased in certain circumstances

Data Subjects have a right to request that certain Personal Data held by MOPAC is erased. This is also known as the right to be forgotten. This is not a blanket right to require all Personal Data to be deleted. The right will be triggered in any of the following circumstances:

- if MOPAC is continuing to process Personal Data beyond the period when it is necessary to do so for the purpose for which it was originally collected;
- if MOPAC is relying on consent as the legal basis for processing and the Data Subject withdraws their consent;
- if MOPAC is relying on legitimate interest as the legal basis for processing and the Data Subject objects to this processing and there is no overriding compelling ground which enables MOPAC to continue with the processing;
- if the Personal Data has been processed unlawfully (i.e. in breach of the requirements of the GDPR); or
- if it is necessary to delete the Personal Data to comply with a legal obligation.

There are some exemptions to the right to erasure, so even if one of the triggers above is met it may not be necessary to erase the relevant information. If information is required to exercise or defend legal claims, then it is not necessary to delete the Personal Data. MOPAC is also permitted to retain Personal Data where there is a public interest task which requires the Personal Data to continue to be processed or for research purposes.

Right to restrict processing of Personal Data in certain circumstances

Data Subjects have a right to block the processing of their Personal Data in certain circumstances.

The right will be triggered in any of the following circumstances:

- if the Data Subject is disputing the accuracy of Personal Data, then processing of that data should be restricted whilst MOPAC is verifying the accuracy of the Personal Data;
- if the Data Subject has raised an objection to processing, then processing should be restricted whilst MOPAC is considering whether the objection should be upheld;
- if processing of Personal Data is unlawful and the Data Subject opposes erasure and requests restriction instead; or
- if the Personal Data is no longer required by MOPAC but the Data Subject requires the Personal Data to be retained to establish, exercise or defend a legal claim.

If a request to restrict processing is made, then it will be necessary for MOPAC to determine whether the request should be upheld and whether procedures need to be put in place to restrict the use of the relevant Personal Data. If the request to restrict processing is not upheld, then the Data Subject needs to be notified of the reasons for this.

Right to data portability

In certain circumstances Data Subjects can request to receive a copy of their Personal Data in a commonly used electronic format. This right only applies to information that Data Subjects have provided to MOPAC (for example by completing a form or providing information through a website). In addition, if information about a Data Subject has been gathered by monitoring their activities then this information will also be subject to the right to data portability. However, any analysis done by MOPAC in relation to the Data Subject would not constitute information that they have provided to MOPAC and therefore is not subject to the right of data portability.

The right to data portability only applies if the processing that MOPAC is carrying out is based on the Data Subject's consent or if the information must be processed for the performance of a contract. In addition, the right only applies in relation to data processing that is carried out by automated means (i.e. electronically).

In order to provide the data in response to a portability request the data must be provided in a commonly used and machine-readable form.

The Data Subject also has a right to request that the data is transferred directly to another organisation. If this is technically feasible, then MOPAC must comply with such a request.

Right to object to processing of Personal Data in certain circumstances, including where Personal Data is used for marketing purposes

Data Subjects have a right to object to data processing being carried out by MOPAC in certain circumstances.

The right will be triggered in any of the following circumstances:

- if MOPAC is processing data based on legitimate interests or for the performance of a task in the public interest (including profiling);
- if MOPAC is using Personal Data for direct marketing purposes; or
- if information is being processed for scientific or historical research or statistical purposes.

If an objection is raised in relation to Personal Data that is being processed on a legitimate interest or public interest ground, then a balancing test must be carried out to consider whether there are any compelling legitimate grounds which enable MOPAC to continue processing the data. In each case the outcome of this decision and the reasons for it must be documented.

If an objection is raised in relation to direct marketing, then the objection must be upheld, and no balancing test will be carried out.

Data Subjects must be informed that they have a right to object at the point of data collection and the right to object must be explicitly brought to the attention of the Data Subject and be presented clearly and separately from any other information.

If you receive an objection to marketing, you must ensure that you stop any marketing to that Data Subject as soon as possible.

Right not to be subject to automated decisions where the decision produces a legal effect or a similarly significant effect

Data Subjects have a right not to be subject to a decision which is based on automated processing where the decision will produce a legal effect or a similarly significant effect on the Data Subject.

There are exemptions from this prohibition if the decision is necessary to enter into or perform a contract with the Data Subject, is authorised by law or is based on explicit consent.

If one of these exemptions applies, then it is still necessary to inform the Data Subject of the automated decision making and provide them with an opportunity to object and request manual intervention.

If any automated decisions are being made, then it will be necessary for MOPAC to analyse whether the decision has a legal effect or a similarly significant effect. If so, then advice should be sought from the DPO in relation to the steps that need to be taken to ensure that the automated decision making is carried out in a compliant way.

It is our policy to respect the rights of Data Subjects and MOPAC will act promptly and in accordance with data protection laws should any of these rights be exercised. [For more details about how to respond to any of these requests See MOPAC's Data Subjects Right Policy for more information.]

What must MOPAC do to comply when responding to data subject rights under the GDPR?

MOPAC must put in place processes in order to ensure that when Data Subject wishes to exercise any of their rights under GDPR the correct procedure is followed.

All employees at MOPAC must be trained to ensure that they can recognise Data Subject's rights when they are raised.

MOPAC will respond to a request promptly and in any event within one month of receiving it. The rights are not absolute and in some cases MOPAC will apply certain exemptions before complying with the relevant request. If you receive such a request, please contact James Bottomley immediately at james.bottomley@mopac.london.gov.uk.

5. Direct marketing

When MOPAC uses Personal Data for electronic marketing purposes, MOPAC makes sure that those who receive the marketing information have given prior consent. unless MOPAC can rely on any exemptions under any laws and/or regulations relating to marketing, such as soft opt-in, which can be used when MOPAC has obtained the individual's contact details through the performance or negotiation of the provision of goods or services.

In particular, MOPAC adheres to the following principles:

- Data Subjects can opt out of marketing at any time, for example by clicking on any unsubscribe link included in marketing communications or emailing us directly;
- there is no charge for opting out; and
- it is as easy to withdraw consent as it was to provide consent for direct marketing.

- Each marketing communication must provide contact details of the Controller and clear information to enable individuals to opt out. A clear explanation of what MOPAC does with the Personal Data must be included with the communication.

6. Sharing Personal Data with Third Parties

When MOPAC collects Personal Data from Data Subjects, MOPAC must be clear and open about whether it is going to share the Personal Data with Third Parties or not. If MOPAC is going to share Personal Data with Third Parties, they must explain (for example, in the privacy notices) why it needs to do this.

Where Data Subjects would reasonably expect MOPAC to share Personal Data, then MOPAC will be permitted to do so, provided that the data sharing is for a legitimate business purpose.

MOPAC must only use Third Party processors that provide sufficient guarantees to implement appropriate measures to ensure that the requirements of GDPR and the rights of individuals are met. In addition, arrangements with Third Parties must be documented in a written contract and that contract must include mandatory clauses as set out in the GDPR. MOPAC must also carry out checks on Third Parties to ensure that they are compliant with applicable requirements. .

MOPAC must put in place procedures to carry out ongoing monitoring of Third Party processors to ensure compliance with data protection requirements.

If MOPAC wishes to pass Personal Data to a Third Party for the purposes of any marketing activity that is not carried out by MOPAC or in its name, then MOPAC must make sure that it has express consent from the Data Subject to do this.

7. Transferring Personal Data overseas

MOPAC cannot send Personal Data, or allow people to access Personal Data, outside the European Economic Area (EEA). If you believe there is a requirement for data to leave the EEA please contact your DPO.

8. Special Categories of Personal Data

Where MOPAC processes and holds Special Category Data and criminal offence data; such information will always be kept to a minimum, with restricted access permissions, and will be kept for such periods as are set out in the Data Retention Policy. Special Category Data and criminal offence data will only be used for the purposes for which it was captured or provided as set out in the relevant privacy notice.

A summary of how MOPAC processes Special Category Data and criminal offence data is set out below:

i. **Racial or ethnic origin: May be used for segmentation of survey or crime data. Held on secured system in areas of the file structure with limited access and are password protected.**

ii. **Political affiliations or opinions: MOPAC would not process such data.**

iii. **Criminal offence data: May be processed for evaluation of MOPAC services. Would not be removed from the MPS system which is a secure system.**

iv. **Religious or philosophical beliefs: MOPAC would not process such data.**

v. **Trade union membership: Held by the TU on MOPAC systems. Can only be viewed by TU.**

vi. **Genetic data: MOPAC would not process such data.**

vii. **Biometric data: MOPAC would not process such data.**

viii. **Physical or mental health conditions: MOPAC holds such data in a secured area which is only accessible to HR staff.**

ix. **Sexual lifestyles or sexual orientation: Only held in anonymised format.**

Disclosing Special Category Data and criminal offence data

The processing and disclosure of Special Category Data or criminal offence data may cause profound distress to individuals. **All such disclosures are prohibited unless all of the following criteria are met**:

A MOPAC has identified that the individual making the request for access to Special Category Data/criminal offence data has a legitimate and clearly identified need to access to the data;

B MOPAC has, at the time of its collection, made clear how Special Category Data/criminal offence data would be processed, that the Third Parties who would have access to the Special Category Data/criminal offence data and the circumstances in which such disclosure would be likely to arise; and

C before disclosing the Special Category Data/criminal offence data, MOPAC has obtained the explicit written consent from the individual concerned, where appropriate.

9. Data protection by design and data protection by default

In relation to its obligations under the GDPR, as set out in this policy, MOPAC must ensure that compliance with such obligations is integrated by design and by default into MOPAC's operations, by implementing appropriate measures designed to (without limitation, but in each case taking into account the state of the art, costs of implementation, the nature of data processing and the risks to individuals):

- implement pseudonymisation or anonymisation, as appropriate;
- ensure that only the minimum amount of Personal Data is collected and stored;
- ensure that, when new projects are commenced, data protection by design and by default principles are embedded in the project methodology from the

outset; where the associated processing is likely to result in a high risk to the rights and freedoms of individuals, to consider privacy issues from the project's outset by conducting DPIAs. See Section [ ] (*Data protection impact assessments*) for more details; and

- ensure that, when procuring goods or services from Third Party processors due diligence is carried out on how those processors ensure data protection by design and by default.

10. Data Protection Impact Assessments

Where the nature of the Processing of Personal Data poses a high risk to Data Subjects. DPIAs must be completed prior to any Processing being carried out. Once in place, a DPIA should be re-visited annually to check if there have been any changes to the Processing activity, the documented risks or the controls in place.

MOPAC has a DPIA Procedure in place:

- DPO to be consulted in relation to DPIAs;
- all new projects to be assessed using the DPIA Checklist to determine whether there is any high-risk data processing operation involved and, therefore, whether a DPIA is required;
- a DPIA to be conducted prior to commencement of the proposed processing for all projects where the processing is likely to result in a high risk to the rights and freedoms of Data Subjects involving Personal Data;
- implementation of mitigating actions identified in a DPIA as necessary to remove high risks from the project; and
- in cases where a high risk cannot be removed from the project, the employee conducting the DPIA is to consult with the DPO, to enable them to consult with the relevant SA, if appropriate.

If a DPIA is not required because the project is not high risk, but the project does involve the Processing of Personal Data you must complete a Privacy Review instead of a DPIA.

11. Records

MOPAC must keep and maintain a ROPA which details the below information:

- the name and contact details of the controller and, where applicable, any joint controller, the controller's representative and the data protection officer;
- Categories of Personal Data;
- Purpose of processing;
- Legal basis for processing;
- Third Parties the Personal Data who you are sharing the Personal Data with;
- Details of any transfers outside of the EEA;

- Retention periods for the Personal Data; and
- General description of security measures in place to protect the Personal Data.

Any new data processing activities or changes to existing data processing activities must be recorded on the ROPA and MOPAC must put in place a process to regularly review the record to ensure that it is accurate and up to date.

DPIAs are used to help identify when the record needs to be updated.

12. Keeping Personal Data secure

MOPAC takes reasonable technical and organisational precautions to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, by:

- protecting Personal Data held in hardcopy or electronic form;
- ensuring that information containing Personal Data and in Particular any Special Category Data/criminal offence data, will be handled appropriately; and
- making sure that Personal Data is not transferred outside the EEA without suitable safeguards.

In particular you must:

- take steps to prevent the accidental, improper or deliberate disclosure, misuse or loss of Personal Data and prevent unauthorised access to it;
- limit the disclosure and access to Personal Data to those who have a business need to access it and
- not disclose Personal Data relating to Data Subjects without a lawful reason to do so.

13. Personal Data breaches

If a Personal Data breach occurs, unless the breach is low risk to the Data Subject, MOPAC must notify the Personal Data breach to relevant SA. If the Personal Data breach could pose a significant risk to the Data Subjects, then they must also be notified of the Personal Data breach. Notification of the Personal Data breach, to the relevant SA, must take place within 72 hours of upon MOPAC becoming aware of the Personal Data breach. Notification to Data Subjects must happen without undue delay.

MOPAC must put in place procedures to ensure that as soon as any employee becomes aware of a Personal Data breach it is escalated to the DPO immediately by email at james.bottomley@mopac.london.gov.uk. The DPO will review the nature of the Personal Data breach, carry out an investigation and determine whether the Personal Data breach needs to be notified to the SA or to Data Subjects.

Under no circumstances should anyone at MOPAC other than the DPO notify any SA of a Personal Data breach.

MOPAC must maintain a log of all Personal Data breaches and make this log available to the relevant SA upon request.

Despite all MOPAC's best efforts, issues may sometimes arise.

For example:

- MOPAC may lose Personal Data accidentally;
- An e-mail is sent to wrong recipient;
- someone may steal Personal Data or attack MOPAC systems;
- an employee at MOPAC may not be authorised to use Personal Data; or
- MOPAC's IT equipment may fail.

In the case of a Personal Data breach, MOPAC need to act quickly and appropriately to manage the Personal Data breach and limit the effects and damage it causes.

If you suspect or become aware of a Personal Data breach, please follow the steps set out in the Data Breach Policy to enable MOPAC to respond appropriately.

Consequences

Personal Data breaches can have consequences in terms of real harm and distress Data Subjects. Personal Data breaches can also lead to serious consequences for MOPAC's reputation and could lead to a serious loss of trust.

In addition, SAs have the power to take legal enforcement action where organisations breach data protection legislation. This includes the ability to impose large fines.

Data Subjects may also be able to claim compensation from MOPAC if we suffer a breach that puts their Personal Data at risk.

14. Training

MOPAC will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests, will receive additional training to help them understand their duties and how to comply with them.

15. Audit

DARA will monitor and report on compliance with the policy and all relevant data protection legislation.

16. Complaints

Under the policy, MOPAC will treat any complaint about our processing of Personal Data as a matter of urgency. MOPAC can be notified of a complaint by email at enquiries@mopac.london.gov.uk.

17. Policy updates

We will review this Policy and the associated documents periodically and will make any updates deemed necessary. You will be required to comply with any updates made from the date the updated policy is made available to employees.

Document version history

The following table details a record of the changes made to this document:

Version	Date	Author	Description of change
0.1	27/02/2020	James Bottomley	First draft

16. Associated polices

- DPIA Policy
- Information Security Policy
- FOI Policy
- SAR Policy
- Cyber Security Policy
- MOPAC Code of Conduct
- Retention and Review Policy

All held within S:\GDPR\02 Policies and Procedures