Data Protection Policy (UK GDPR Version)

VERSION 5 APRIL 2024

This policy sets out the Combined Authorities' commitment to data protection and individual rights in relation to personal data and sensitive personal data.

Document Control:

Version	Date	Brief Summary of Changes	Author
0	R Jackson	Initial Draft	07//02/2018
0	C James	Reviewed and minor amends	07/05/2018
0	C James	Incorporated comments from S Davenport	22/05/2018
0	C James	Further minor amends to 7.4 and 9.1	25/05/2018
0	R Jackson	Added DPA 2018 info	03/08/2018
1	R Jackson	Final version	03/08/2018
1.1	L Gandy	Annual review	25/11/2019
2	L Gandy	Annual review	1/02/21
3	C James	Name change review	15/09/21
4	C James	SIRO and Asset Owners update	18/03/22
5	K Hopkins	Annual review. SIRO updated and minor amendments.	23/04/2024

Document Approval

Approving Body or Person	Role (review, approve)	Date
Senior Management Team Meeting	Approve	07/01/20
DPO		

Contents

This Policy may be amended as and when further guidance is published by the Information Commissioner's Office or other relevant official body.

DEFINITIONS:

Automated Decision-Making: when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the UK GDPR/DPA. We are the Controller of all Personal Data relating to South Yorkshire Mayoral Combined Authority (SYMCA) Personnel and Personal Data used in our business for our own purposes.

Criminal Convictions Data: means Personal Data relating to criminal convictions and offences and includes Personal Data relating to criminal allegations and proceedings.

Data Protection Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should always be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the UK GDPR, being the Director of Legal and Governance for South Yorkshire Mayoral Combined Authority.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

Information Asset Owners: senior responsible individuals, namely the Assistant Directors/Heads of Departments, as nominated by the Senior Information Responsible Officer to understand what information is held, added, removed, moved, accessed and to address information risks and ensure information is held and used within the law for public good and in a manner to ensure compliance with the UK GDPR/DPA.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR/DPA.

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when SYMCA collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms (e.g. key coding) so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: SYMCA's policies, guidance, operating procedures or processes related to this Policy and designed to protect Personal Data.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

SYMCA Personnel: all employees, workers, contractors, agency workers, consultants, directors, members and others.

UK GDPR (General Data Protection Regulation): the General Data Protection Regulation (*(EU) 2016/679*) *as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018*. Personal Data is subject to the legal safeguards specified in the UK GDPR (as incorporated and tailored by the Data Protection Act 2018 (DPA) in the UK) and as amended by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019).

1. INTRODUCTION

1.1 This Data Protection Policy ('Policy') sets out how South Yorkshire Mayoral Combined Authority ("we", "our", "us", "SYMCA") handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

1.2 This Policy applies to all Personal Data we Process regardless of the media (and includes paper as well as electronic data) on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

1.3 This Policy applies to all SYMCA Personnel ("you", "your"). You must read, understand and comply with this Policy when Processing Personal Data on our behalf and complete/attend training on its requirements. This Policy sets out what we expect from you in order for SYMCA to comply with applicable law. Your compliance with this Policy is mandatory. Related Policies, procedures and guidance are available to help you interpret and act in accordance with this Policy. You must also comply with all such Related Policies, procedures and guidance including;

- Data Breach Management Procedure;
- Data Protection Impact Assessment Procedure;
- Procedure for Managing Requests for Access to Information; **NOTE:** The UK GDPR and DPA 2018 does not apply to requests for information about a person if they are deceased. These requests should be processed in accordance with the Freedom of Information Act 2000 (see Procedure for Managing Requests for Access to Information), and should also be considered fairly and lawfully.
- Information Asset Assurance Process;
- Document Retention Policy (and the related Retention Schedule).

1.4 **Any breach of this Policy or Related Policies, procedures and/or guidance may result in disciplinary action.**

1.5 Where you have a specific responsibility in connection with Processing such as capturing Consent, reporting a Personal Data Breach, conducting a DPIA as referenced in this Policy or otherwise then you must comply with the Related Policies and guidance.

1.6 Managers are required to ensure that the service areas for which they are responsible have in place adequate guidance on data protection and effective measures to comply with this Policy.

1.7 This Policy (together with Related Policies, procedures and guidance) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

2. SCOPE

2.1 We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. We are exposed to significant fines for failure to comply with the provisions of the UK GDPR/DPA.

2.2 We also recognise that data in its wider sense, not just Personal Data, must be protected and managed properly to avoid loss of data, potential breaches of confidentiality and reputational damage and potential civil action for breach of contract.

2.3 The Data Protection Officer (DPO) is responsible for overseeing this Policy and, as applicable, developing Related Policies, procedures and guidance. That post is held by Stephen Davenport, Director of Legal and Governance, Steve.Davenport@southyorkshire-ca.gov.uk.

2.4 SYMCA has also appointed Nick Brailsford, Head of Digital Transformation, as the Senior Information Risk Owner (SIRO), Nick.Brailsford@southyorkshire-ca.gov.uk.

2.5 Please contact the DPO or SIRO with any questions about the operation of this Policy or the UK GDPR/DPA or if you have any concerns that this Policy is not being or has not been followed. In particular, you must always contact the DPO or SIRO in the following circumstances:

a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by SYMCA) (see *Paragraph 4.1* below);

b) if you need to rely on Consent and/or need to capture Explicit Consent (see *Paragraph 4.2* below);

c) if you need to draft Privacy Notices (see *Paragraph 4.3* below);

d) if you are unsure about the retention period for the Personal Data or other data being Processed (see *Paragraph 8* below);

e) if you are unsure about what security or other measures you need to implement to protect Personal Data and other data (see *Paragraph 9.1* below);

f) if there has been a Personal Data Breach or suspected Personal Data Breach (*Paragraph 9.2* below or a loss of other data or potential breach of any data sharing agreement or other issue relating to data) contact must be made immediately due to the requirement to notify the Information Commissioner's Office (ICO) within 72 hours of SYMCA becoming aware of the breach;

g) if you are unsure on what basis to transfer Personal Data outside of the UK (see *Paragraph 10* below);

h) if you need any assistance dealing with any rights invoked by a Data Subject (see *Paragraph 11*);

i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see *Paragraph 12.4* below) or plan to use Personal Data for purposes others than what it was collected for. It should be noted that this includes new or changes to IT systems/processes.

j) If you need help complying with applicable law when carrying out direct marketing activities (see *Paragraph 12.6* below); or if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see *Paragraph 12.7* below).

k) if you need advice about data security or other data issues.

3. PERSONAL DATA PROTECTION PRINCIPLES

3.1 We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR (Article 5)/DPA (sections 35-40) which require Personal Data to be:

a) processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

b) collected only for specified, explicit and legitimate purposes and not further processed in a manner that is not incompatible with those purposes (Purpose Limitation).

c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

d) accurate and where necessary kept up to date (Accuracy).

e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).

f) processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

g) not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and

h) made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

3.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

4. LAWFULNESS, FAIRNESS, TRANSPARENCY

4.1 LAWFULNESS AND FAIRNESS

4.1.1 Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

4.1.2 You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The UK GDPR/DPA restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

4.1.3 The UK GDPR/DPA allows Processing for specific purposes, some of which are set out below:

a) the Data Subject has given his or her clear Consent to process their Personal Data for one or more specific purposes;

b) the Processing is necessary for the performance of a contract with the Data Subject or because they have asked you to take steps before entering into a contract;

c) the Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in SYMCA;

d) to meet our legal compliance obligations;

e) to protect the Data Subject's vital interests;

f) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests are set out in SYMCA's Privacy Notices on its website.

4.1.4 You must identify and document the legal ground being relied on for each Processing activity.

4.2 CONSENT

4.2.1 SYMCA must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR/DPA, which include Consent.

4.2.2 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

4.2.3 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

4.2.4 **Unless we can rely on another legal basis of Processing, Explicit Consent is usually required.**

4.2.5 When Processing Special Categories of Personal Data and Criminal Convictions Data we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

4.2.6 You will need to evidence Consent captured and keep records of all Consents in accordance with Related Policies and privacy guidance so that SYMCA can demonstrate compliance with Consent requirements.

4.3 TRANSPARENCY (NOTIFYING DATA SUBJECTS)

4.3.1 The UK GDPR/DPA requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them. You must check with the SIRO that your Privacy Notices are adequate.

4.3.2 Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR/DPA including the identity of the Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

4.3.3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with all the information required by the UK GDPR/DPA as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the UK GDPR/DPA and on a basis which contemplates our proposed Processing of that Personal Data.

4.3.4 If you are collecting Personal Data from Data Subjects, directly or indirectly, then you must provide Data Subjects with a Privacy Notice in accordance with our Related Policies and privacy guidance. You must check with the SIRO that your Privacy Notices are adequate.

5. PURPOSE LIMITATION

5.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

5.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

6. DATA MINIMISATION

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

6.2 You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

6.3 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

6.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with SYMCA's data retention guidelines.

7. ACCURACY

7.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

7.2 You will ensure that the Personal Data we use, and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

8. STORAGE LIMITATION

8.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

8.2 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

8.3 SYMCA will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with SYMCA's policy on data retention.

8.4 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with SYMCA's policy on data retention. This includes requiring third parties to delete such data where applicable.

8.5 You will ensure Data Subjects are informed of the period for which data is stored and how that period is detailed in any applicable Privacy Notice.

8.6 For non-Personal Data you should only retain data for as long as necessary and in accordance with any application periods set out in the SYMCA's policy on data retention.

9. SECURITY INTEGRITY AND CONFIDENTIALITY

9.1 PROTECTING PERSONAL DATA AND OTHER DATA

9.1.1 Personal Data and non-Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

9.1.2 We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories

of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

9.1.3 More widely you should apply similar protection to non-Personal Data that is commercially valuable or sensitive.

9.1.4 You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested. You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

9.1.5 You must comply with all applicable aspects of our information security policies and comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR/DPA and relevant standards to protect Personal Data.

9.2 REPORTING A PERSONAL DATA BREACH

9.2.1 The UK GDPR/DPA requires Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

9.2.2 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

9.2.3 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO (Data.ProtectionOfficer@SouthYorkshire-CA.gov.uk) and SIRO to enable reporting to the Information Commissioners Office within 72 hours if required and follow the Data Breach Management Procedure. You should preserve all evidence relating to the potential Personal Data Breach.

10. TRANSFER LIMITATION

10.1 The UK GDPR/DPA restricts data transfers to countries outside the UK in order to ensure that the level of data protection afforded to individuals by the UK GDPR/DPA is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

10.2 You may only transfer Personal Data outside the UK after consultation and written approval of the DPO and SIRO.

10.3 NO DATA TRANSFERS OUTSIDE OF THE UK SHOULD BE UNDERTAKEN WITHOUT THE EXPLICIT CONSENT OF THE DPO OR SIRO.

11. DATA SUBJECT'S RIGHTS AND REQUESTS

11.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

a) withdraw Consent to Processing at any time;

b) receive certain information about the Data Controller's Processing activities;

c) request access to their Personal Data that we hold (see Data Subject Access Request Procedure);

d) prevent our use of their Personal Data for direct marketing purposes;

e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data (SYMCA will do this within one month of receiving the request for rectification);

f) restrict Processing in specific circumstances;

g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

h) request a copy of an agreement under which Personal Data is transferred outside of the UK;

i) object to decisions based solely on Automated Processing, including profiling and Automated Decision-Making (ADM);

j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

l) make a complaint to the supervisory authority; and

m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

11.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

11.3 You must immediately forward any Data Subject Access Request you receive to the DPO and comply with SYMCA's Procedure for Managing Requests for Access to Information.

12. ACCOUNTABILITY

12.1 THE DATA CONTROLLER

12.1.1 The Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles. SYMCA must have adequate resources and controls in place to ensure and to document UK GDPR/DPA compliance including:

a) appointing a suitably qualified DPO;

b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

c) integrating data protection into internal documents including this Policy, Related Policies, privacy guidance or Privacy Notices;

d) regularly training employees on the UK GDPR/DPA, this Policy, Related Policies, procedures and guidance. SYMCA shall maintain a record of training attendance by employees; and

e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

12.2 RECORD KEEPING

12.2.1 The UK GDPR/DPA requires us to keep full and accurate records of all our data Processing activities.

12.2.2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

12.2.3 These records should include, at a minimum, the name and contact details of the Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps/information asset registers should be created which should include the detail set out above together with appropriate data flows.

12.2.4 Certain posts within SYMCA will be designated as Information Asset Owners and in accordance with the Information Asset Assurance Process, these post holders will be responsible for creating, reviewing (at least annually) and maintaining the data maps/information asset registers.

12.3 TRAINING AND AUDIT

12.3.1 We are required to ensure all employees have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

12.3.2 You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training when required by the organisation.

12.3.3 You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

12.4 PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

12.4.1 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

12.4.2 You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

a) the state of the art;

b) the cost of implementation;

c) the nature, scope, context and purposes of Processing; and

d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

12.4.3 Data Controllers must ensure that DPIAs are conducted in respect to high risk Processing. DPIAs will be conducted by the Information Asset Owners who must then update the Information Asset Register.

12.4.4 You should always conduct a DPIA (and discuss your findings with the DPO and SIRO) when implementing major system or business change programs involving the Processing of Personal Data including:

a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

b) Automated Processing including profiling and ADM;

c) large scale Processing of Special Categories of Personal Data or Criminal Convictions Data; and

d) large scale, systematic monitoring of a publicly accessible area.

In accordance with ICO guidance it is recommended that a DPIA is carried out even where there is no legal obligation as the DPIA process can be used as a flexible and scalable tool to suit any project and to help assessment of risks in any planned data sharing.

12.4.5 A DPIA must include:

a) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

c) an assessment of the risk to individuals; and

d) the risk mitigation measures in place and demonstration of compliance.

You must comply with any SYMCA guidance on DPIA and Privacy by Design.

12.5 AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING (ADM)

12.5.6 Automated Processing and Automated Decision-Making must not take place without the specific consent of the DPO and SIRO.

12.6 DIRECT MARKETING

12.6.1 We are subject to certain rules and privacy laws when marketing to our customers.

12.6.2 For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

12.6.3 The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

12.6.4 A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

12.7 SHARING PERSONAL DATA

12.7.1 Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

12.7.2 You may only share the Personal Data we hold with another employee, agent or representative of SYMCA if the recipient has a job-related 'need to know' basis for the information and the transfer complies with any applicable cross-border transfer restrictions.

12.7.3 You may only share the Personal Data we hold with third parties, such as our service providers if:

a) they have a need to know the information for the purposes of providing the contracted services;

b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

d) the transfer complies with any applicable cross border transfer restrictions; and

e) a fully executed written contract that contains UK GDPR/DPA approved third party clauses has been obtained; and

f) a data sharing agreement is completed if deemed necessary by the DPO and/or SIRO.

12.7.4 For non-Personal Data sharing should only take place with third parties where appropriate contractual arrangements are in place approved by the Legal Department.

13. INFORMATION COMMISSIONER – NOTIFICATION AND REGISTRATION

13.1 SYMCA has registered its use of personal data with the Information Commissioner and the register references are given below. The registers can be accessed and searched on the Information Commissioner's website: http://www.ico.org.uk.

13.2 Data Controller: South Yorkshire Mayoral Combined Authority
Registration Ref: ZA092329

13.3 SYMCA will review the Data Protection Registration annually and notify the Information Commissioner of any amendments.

14. CHANGES TO THIS POLICY

14.1 We reserve the right to change this Policy at any time so please check back regularly to obtain the latest copy of this Policy. This policy will be reviewed at least every 24 months or earlier as deemed necessary by the DPO. Changes to the Policy will be communicated to employees.

14.2 For and on behalf of South Yorkshire Mayoral Combined Authority

…… ……
Chief Executive Date