Data Protection Policy

December 2024

Contents

1. Introduction

1.1 SW9 CH understands the importance of protecting its residents, staff, and visitor's data. This policy outlines how SW9 CH will govern the processing of personal data and its compliance with data protection legislation.

1.2 The Data Protection Act 2018 (DPA) sits alongside The UK General Data Protection Regulation (GDPR UK). It applies to personal data (data that allows any living individual to be identifiable) that is:

- Held on a computer or any other automated system (including e-mails, documents, data on mobile phones, iPads etc.).
- Held in a relevant filing system (a paper system such as client records system, or a set of files on service users that is organised alphabetically by the name of the person or some other identifier such as case number); or
- Intended to go onto computer or into a relevant filing system.

1.3 According to the Information Commissioners Office, personal data will be protected under the regulations if it is information that:

- Is being processed by means of equipment operating automatically in response to instructions given for that purpose.
- Is recorded with the intention that it should be processed by means of such equipment.
- Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.
- Is recorded information held by a public authority.
- Is held on computer or is intended to be held on computer. So, data is also information recorded on paper if you intend to put it on computer.

1.4 Where the above processing refers to data collected prior 31 December 2020 or the processing takes place within the European Union, then SW9 CH will ensure it complies with Regulation 2016/679 (EU GDPR).

2. Aims and objectives

2.1 The purpose of this policy is to enable SW9 CH to:

- Comply with the Data Protection Act (2018) and UK GDPR in respect of the personal data it uses
- Follow Good Data Management Practice.
- Protect SW9 CH's residents, staff, and partners through commitment to privacy protection
- Reduce the risk of breaching Data Protection Compliance
- Protect the organisation from the consequences of a breach of Data Protection Compliance

3. Definitions

3.1 **"Data" is** information that is a) processed by means of equipment operating automatically in response to instructions given for that purpose, b) recorded with the intention that it should be processed by means of such equipment, c) recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.

3.2 **"Data subjects"** is an individual who is the subject of Personal data. Data subjects have legal rights in relation to the handling and processing of their Personal data.

3.3 **"Personal data"** is any data which relates to an individual who can be identified a) from that data or, b) from that data and other information in our possession or likely to come into our possession. Personal data can be factual (i.e. name, address, or date of birth) or an opinion (e.g. performance appraisal).

3.4 **"Data Controller"** is a person who (either alone or jointly with other persons) determines the purposes for which, and the manner in which, any Personal data is to be processed. They have a responsibility to establish practices and policies in line with the appropriate data protection legislation.

3.5 **"Data Owner"** is accountable for who has access to information within their service area.

3.6 **"Data users"** are all employees whose work involves the use and or processing of Personal data. Data users have a duty to protect the information they handle by following and adhering to the Data Protection and Information Security policies at all times.

3.7 **"Data processors"** is any person, other than an employee of the Data Controller who processes Personal data on behalf of a Data Controller, i.e. third parties that process or handle Personal data on our behalf.

3.8 **"Processing"** is any activity that involves 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, erasure or destruction. Processing also includes transferring Personal data to third parties.

3.9 **"Special Category Personal Data (Sensitive Personal data)"** includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, biometric data processed solely to identify a human being, trade union membership, physical or mental health related data, sexual orientation or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive Personal data can only be processed under strict conditions, and usually requires the express consent of the data subject.

3.10 **"Relevant filing system"** is any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured,

either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

3.11 It is intended to cover non-automated records that are structured in a way which allows ready access to information about individuals. As a broad rule, we consider that a relevant filing system exists where records relating to individuals (such as personnel records) are held in a sufficiently systematic, structured way as to allow ready access to specific information about those individuals

3.12 **"Data Protection Legislation"** refers to the Data Protection Act 2018 and UK GDPR. This also applies to EU GDPR where data is processed in the EU territory or processed before the UK GDPR effective date of 1 January 2021.

4. Policy statement

4.1 The scope of this policy applies to all employees and any third party or individual, who conducts work on behalf of SW9 CH. This policy requires compliance with the appropriate data protection legislation in relation to all Personal data (including Sensitive Personal data) that we process.

4.2 SW9 CH will ensure compliance to protecting personal data by:

- complying with both the law and good practice;
- respecting an individual's rights;
- being open and transparent with an individual whose data isheld;
- providing training and support for staff who handle personal data
- ensuring that sufficient resources are available so that the provisions of data protection legislation can be met;
- ensuring that policies and procedures that involve the processing of personal data support compliance with data protection legislation.
- keeping information securely in the right hands, and
- holding good quality information

5. Safeguarding Individuals

5.1 SW9 CH recognises that its priority under the appropriate data protection legislation is to avoid causing harm to individuals. SW9 CH therefore commits to keeping information securely in the right hands and holding good quality information.

5.2 This policy aims to address the following risks related to the use of personal data:

- Breach of confidentiality (information being given out inappropriately);
- Insufficient clarity about the range of uses to which data will be put, leading to Data Subjects being insufficiently informed.
- Breach of security through unauthorised access, theft, or loss of computer equipment.
- Failure to establish efficient systems of managing changes to data, leading to personal

data being not up to date.

- Harm to individuals if personal data is not up to date.
- Data Processor contracts being unclear about their responsibilities.
- Data not being properly identified and catalogued, as per SW9 CH's statutory obligations.

6. Data Protection Principles

6.1 All processing of personal data must be done in accordance with the following data protection principles, and SW9 CH's policies and procedures are designed to ensure compliance with them. There are six principles that cover issues including the processing, accuracy, security, and lawfulness of data collection as well as the rights of the Data Subject as follows:

- Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.
- Data must be adequate, relevant, and limited to what is necessary.
- Data must be collected for specified, explicit and legitimate purposes and not further processed in as manner that is incompatible with these purpose (subject to exceptions).
- Data must be accurate and, where necessary, kept up to date; reasonable steps must be taken to remove inaccurate information.
- 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 is processed.
- Data must be processed in a manner than ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage.

7. Transparency

7.1 SW9 CH will ensure transparency with easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms". Information will be communicated to Data Subjects in an intelligible form using clear and plain language.

8. Fair and Lawful Processing

8.1 SW9 CH is committed to ensuring that the processing of Personal Data in its organisation is done fairly and without adversely affecting the rights of the Data Subject.

8.2 SW9 CH will endeavour to inform the Data Subjects of the purpose for which the data is to be processed and any sharing with third parties to whom the personal data may be disclosed or transferred.

8.3 Personal data may only be processed for the specific purpose notified to the Data Subject when it was first collected, or for purposes specifically permitted by Data Protection Legislation. Personal data must not be collected for one purpose and subsequently used for another. If it becomes necessary to change the purpose for which the data is being processed, the Data Subject must be informed of the new purpose before any processing occurs.

8.4 SW9 CH's Data Protection Officer is to ensure that procedures are developed throughout the company as appropriate to ensure that Individuals who supply the company with Personal data are provided with a 'Privacy or Fair Processing Notice' (or online privacy statement) which communicates the following:

- The identity of the organisation.
- The purpose(s) for which Personal data will be processed.
- Information regarding the disclosure of Personal data to third parties.
- Information regarding the individuals' right of access to Personal data.
- Whether Personal data is transferred outside the UK.
- How to contact the company with questions or queries regarding the processing of Personal data.
- Details of specific technologies or electronic measure to collect information about individuals, e.g. website cookies.

9. Processing of Special Categories of Data and Data related to Criminal Convictions

9.1 Where special categories of data are processed, the organisation will only undertake such processing with a valid lawful basis and special condition. If consent is applicable, SW9 CH will ensure that it is able to be evidenced and obtained in alignment with the data protection legislation.

9.2 Where SW9 CH undertakes the processing of personal data relating to criminal convictions and offences, it will only do so with a lawful basis and ensure transparency. Should consent be required, the organisation will ensure consent is obtained in an appropriate manner and explicit in alignment with the appropriate data protection legislation.

9.3 SW9 CH will ensure the necessary security measures and safeguards are in place when undertaking such processing.

10. Data Subject Rights

10.1 SW9 CH will ensure that Data Subject's rights are respected, and that Data Subjects are able to exercise their rights. SW9 CH will ensure that a process for Subject Access Requests (SARs) is created and communicated so that staff can recognise requests, advise the subject on the correct process to be followed, and ensure the request is processed within the legal requirement of one month. SW9 CH will also ensure that:

- Data Subjects can make subject access requests regarding the nature of information held and to whom it has been disclosed.

- They gain consent, where applicable, for sharing and dissemination of personal data for.
- processing with partners.
- They prevent processing likely to cause damage or distress.
- They prevent processing for purposes of direct marketing.
- Data Subjects are informed about the mechanics of any automated decision-taking process that will significantly affect them.
- Data Subjects will not have significant decisions that will affect them taken solely by automated process.
- Data Subjects can sue for compensation if they suffer damage by any contraventionof the data protection legislation.
- Data Subjects can take action to rectify, block, erased (including the right to be forgotten) or destroy inaccurate data.
- Data Subjects can request the ICO to assess whether any provision of the data protection legislation has been contravened.
- Data Subjects have the right for personal data to be provided to them in a structured, commonly used, and machine-readable format, and the right to have that data transmitted to another controller.
- Data Subjects have the right to object to any automated profiling without consent.

11. Review and Communication

11.1 The Data Protection Officer will ensure that, on a biannual basis, all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant, and not excessive. On at least an annual basis, the Data Protection Officer will review all the personal data maintained by SW9 CH by reference to the Records of Processing and Information Asset Register, and will identify any data that is no longer required in the context of the registered purpose and will arrange to have that data securely deleted/destroyed. The Data Protection Officer will also:

- Ensure that all staff receive training in their responsibilities under Data Protection
- Ensure that all staff receives annual 'refresher' training, including modules on Data Protection.
- Disseminate Data Protection related guidance documents and make available for staff to ensure that they conduct their duties in complying with the regulation.

12. Transferring of Personal Data outside of the UK

12.1 SW9 CH will ensure that its processing does not result in personal data being transferred to a country or territory outside the United Kingdom unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data as permitted by appropriate data protection legislation.

12.2 The transfer of personal data outside of the UK is prohibited unless one or more of the specified safeguards or exceptions apply.

12.3 An assessment of the adequacy considering the following factors:

- The nature of the information being transferred.
- The country or territory of the origin, and final destination, of the information.
- How the information will be used and for how long.
- The laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- The security measures that are to be taken as regards the data in the overseas location. (This is a UK-specific option.)

12.4 Binding Corporate Rules – SW9 CH may adopt approved Binding Corporate Rules for the transfer of data outside the UK. This requires submission to the relevant Supervisory Authority for approval of the rules that the organisation is seeking to rely upon.

12.5 Model Contract Clauses – SW9 CH may adopt approved model contract clauses for the transfer of data outside of the UK. If SW9 CH adopts the model contract clauses approved by the relevant Supervisory Authority, there is an automatic recognition of adequacy.

12.6 Exemptions - In the absence of an adequacy decision, including binding corporate rules, a transfer of personal data to a third country, or an international organisation, could take place only on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.
- the transfer is necessary for important reasons of public interest.
- the transfer is necessary for the establishment, exercise, ordefence of legal claims.
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.
- the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.
- A list of countries that satisfy the adequacy requirements of the Commission are published in the Official Journal of the European Union.
- SW9 CH’s data or applications should not be accessed outside of the United Kingdom and European Economic Area (EEA) without the written consent of the SW9 CH’s Executive Director and the SW9 Data Protection Officer.

13. Accountability

13.1 SW9 CH will adhere to the principle of accountability and ensure its organisation takes responsibility for ensuring compliance and equally for demonstrating that each processing operation complies with the requirements of the data protection legislation.

14. Records of Processing and Impact Assessments

14.1 SW9 CH will maintain the necessary documentation of all personal data related processing activities, and implement appropriate security measures, performing DPIAs (Data Protection Impact Assessment) where there may be a high risk to individuals concerned.

14.2 Data owners are responsible for ensuring that their processing activities recorded in the privacy management system are a true reflection of the processing of personal data taking place within the business. A review of the records should be carried out every 12 months or whenever there is a substantial change to the processing activities, whichever is sooner. Data owners can delegate the administration of this responsibility to an appropriate person, but they will maintain the overall responsibility.

14.3 The Data owner will be required to complete a Screening DPIA whenever there is a new or substantial change to a process, asset (system), Data Processor or Joint Controller

14.4 Should the Screening DPIA identify the processing as 'high risk' the Full DPIA process will be initiated with support of the Data Protection Officer.

15. Information Sharing Agreements

15.1 Where SW9 CH shares personal data with any third party, an information sharing agreement, ('Data Processor or Joint Controller Agreement') is to exist as part of a formally documented written agreement or contract.

15.2 Where the other party uses the personal data for its own purposes the agreement or contract will clearly describe the purposes for which the information may be used and any limitations or restrictions on the use of that information. When sharing, no personal data is to be shared without establishing:

- The legality and fairness of the purpose.
- The limiting of information disclosure in accordance with the purpose.
- The inclusion or exclusion of third-party information.
- The processing requirements throughout the information's lifecycle (including transfer, storage, and onward processing.

15.3 SW9 CH will undertake post contract award compliance checks as part of its audits of third parties.

15.4 SW9 CH will develop a security assessment framework to pre-assess partners and suppliers in terms of their organisational information assurance maturity.

16. Sharing data under a legal obligation

16.1 Where the processing of personal data with a third party is required by law, procedures are to ensure that the protocols and controls for the sharing of the data are documented, are in compliance with the relevant law requiring disclosure of personal data, and are regularly reviewed and verified.

17. Accountability for subject access requests

17.1 Although personal data may be processed by third parties, the responsibility for complying with a Subject Access Request will lie with SW9 CH where SW9 CH is the Data Controller or a joint controller.

17.2 Due to the requirement for SW9 CH to provide the information needed in a request within one month, SW9's contracts with third party processors must ensure there are arrangements to guarantee that Subject Access Requests are able to be dealt with promptly.

17.3 SW9 will ensure that its partners, suppliers, and stakeholders comply with data protection principles and information management in accordance with this policy, throughout the supply chain.

18. Data protection leadership

18.1 Network will comply with requirements for prior notifications, or approval from supervisory authorities and maintain the appointment of a Data Protection Officer.

19. Complaints and data protection incidents

19.1 Data Subjects who wish to complain to SW9 CH about how their personal information has been processed may lodge their complaint directly with the Data Protection Officer. Data Subjects may also complain directly to the supervisory authority, which is the Information Commissioner's Office, and the Data Protection Officer. Where data subjects wish to complain about how their complaint has been handled, or appeal against any decision made following a complaint, they may lodge a complaint to the Information Commissioner's Office.

19.2 Only the Data Protection Officer or an authorised delegate should communicate any personal data breaches to the Information Commissioner's Office on behalf of SW9 CH.

19.3 Where a data protection incident has been raised or identified, all employees and any third party or individual, who conducts work on behalf of SW9 CH must report this to the Data Protection Officer through completion of the Data Protection Incident Reporting Form. The Data Protection Officer (or delegated authority) will acknowledge complaints and confirm appropriate actions. Unless formally directed by the Data Protection Officer

in writing, employees should not provide formal responses to the outcome of any reported data protection incidents.

19.4 Where an incident has occurred due to using auto complete in Outlook, employees will be required to switch this functionality off for a period of 12 months after their second incident of this nature within a 24 months period.

20. Retention and disposal of data

20.1 Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) SW9 CH's data retention and data disposal policy and procedures will apply in all cases. Appropriate measures are to be applied to protect the privacy and confidentiality of all Personal data throughout its period of retention within the company. Business managers must ensure that appropriate processes and procedures are applied to ensure the regular backup of data, and that backups can be restored when required, irrespective of the period for which they have been retained.

20.2 SW9 CH is committed to ensuring personal data may not be retained for longer than it is required. Some data will be kept for longer periods than others, but all decisions are to be based upon business requirements. A separate Records Management and Retention Policy exist and provides further guidance as to the retention periods and processes adopted by SW9 CH.

21. Data Security

21.1 As required by the Data Protection Principles, SW9 CH will implement appropriate technical measures and appropriate organisational measures to prevent unauthorised or unlawful processing of Personal data and the accidental loss or destruction of, or damage tothat Personal data.

21.2 The measures align with the basic information security principles of:

- Confidentiality – only those persons specifically authorised can access and/or use the data
- Integrity – the data shall be accurate and relied upon for the purpose for which it is being processed
- Availability –the data will only be provided to authorised persons upon receipt of a validated request

21.3 Everyone with access to personal data pertaining to employees or residents is to ensure that:

- The personal data which they hold, or process is kept securely
- Personal data is not disclosed orally, in writing or in any electronic form to any unauthorised person, either deliberately or accidentally.

21.4 Requests for information must be specific, and the level of checks conducted may

depend on the possible harm and distress which inappropriate disclosure of the information could cause to the individual concerned.

21.5 Requests for information must include clarification of the location and exact nature relevant to the personal data covered by the request. (In some cases, personal data may be difficult to retrieve and collate, reducing the scope of the search may save time and effort.)

22. Roles and Responsibilities

22.1 It is a condition of employment that all employees, contracted third parties and individuals abide by the policies endorsed by SW9 CH.

22.2 Any person, who considers that this policy has not been followed in respect of personal data relating to themselves, or others, is to raise the matter directly with their line manager, or, if the matter cannot be resolved, with the Data Protection Officer or HR. Disciplinary proceedings may follow a breach of this or any other SW9 CH policy.

22.3 This policy is communicated to employees as part of their Induction Training Programme and all staff must undergo refresher training annually thereafter. A formal record of all training is to be retained against the individuals' personal records.

22.4 Staff with day-to-day responsibilities for processing Personal data in any form must be able to demonstrate competence in their understanding of the data protection legislation as well as being able to describe the processes through which this is implemented within the business.

22.5 Third party suppliers that store or process Personal data on behalf of the organisation are designated Data Processors and shall be bound by an Information Sharing Agreement.

22.6 Any questions regarding the interpretation or operation of this policy are to be communicated to the Data Protection Officer.

23. The role of the Data Protection Officer

23.1 SW9 CH Data Protection Office (DPO) is accountable for:

a) Ensuring there are appropriate controls and processes to ensue SW9 CH complies with current legislation relating to Data Protection.

b) Ensuring that appropriate 'fair processing' statements are made when the company, its agents, contractors or service providers collect or process Personal data for which the company is the Data Controller, and that these reflect the purposes for which the information may be used and any other parties to whom the information may be revealed (Principle 1).

c) Ensuring that appropriate controls and processes are in place to make sure

personal data is only obtained for specified and lawful business purposes and is not subsequently processed in a manner incompatible with those purposes (Principle 2).

d) Ensuring that that appropriate controls and processes are in place to require all individuals to provide appropriate consent to their personal data being held and processed if applicable.

e) Ensuring the business conducts periodic reviews of records to verify that the personal data held is:
- adequate, relevant, and not excessive for its purpose (Principle 3).
- accurate and up to date (Principle 4).
- not kept longer than is necessary (Principle 5).
- Ensuring that there are appropriate controls and processes to enable a Data Subject to exercise their rights (Principle 6) through the submission of a Subject Access Request (10.1) regarding their Personal data so that the following requirements are met:
- Verify the identity of the claimant.
- Determining whether the request is restricted to information held for specific purposes.
- Ensuring that Subject Access Requests are processed within one calendar month, collating relevant information, and clarifying what information, if any, is to be provided.

f) Ensuring SW9 CH applies appropriate technical measures and SW9 applies appropriate organisational measures to safeguard against unauthorised or unlawful processing of Personal data and against any accidental loss or destruction of, or damage to, Personal data (Principle 7).

g) Ensuring, that appropriate processes and controls exist for the disposal of systems upon which personal data may have been recorded or stored.

h) Ensure Personal data is not transferred to a country or territory outside the United Kingdom (UK) unless that country or territory guarantees the same or higher level of protection for the rights and freedoms of the data subjects in relation to the processing of Personal data.

i) Keeping the Senior Leadership Team informed of Data Protection issues pertaining to SW9 CH, including any changes in legislation that might impact business processes.

j) Ensuring that training is provided to employees on joining the organisation and annually thereafter and that a record of attendance is maintained.

24. Complying with this policy

24.1 Monitoring compliance - The Data Protection Officer will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and general feedback about business procedures.

24.2 Exceptions - Any exception to the policy must be raised with the Data Protection Officer and where necessary, approved by the Senior Leadership Team in advance of exceptions taking place.

24.3 Violations/Non-Compliance - Unauthorised disclosure of personal data could result in a disciplinary matter that may be considered as gross misconduct. A violation of this Policy as well as any supporting policy documents and operating standards must be treated as an incident and investigated, the findings of which will be handled in accordance with SW9 CH's disciplinary procedures, and could lead to termination of employment, or in the case of third parties, termination of the contractual relationship with the company; in certain circumstances this could give rise to legal proceedings.

25. Related documents

Policies

- Record Management and Retention Policy
- Consent Policy
- CCTV Policy
- Processing Special Category of Personal Data Policy

Procedures

- Subject Access Request Procedure
- Data Breach Procedure
- Handling Physical Data Procedure
- Consent Procedure

26. Legislation and regulation

26.1 The legislation listed in this policy is not intended to cover all legislation applicable to Data Protection. To meet the required Information Commissioner's Office, GDPR requirements and to adhere to all relevant law, SW9 CH will take reasonable measures to ensure compliance with any and all applicable legislation by reviewing policies and procedures and amending them as appropriate. The legislation listed within this policy was considered at the time of the development of this policy, but subsequent primary and secondary legislation, case law and regulatory or other requirements will be considered and the policy reviewed and adopted in accordance with the requirements set out therein, even should such subsequent legislation not be explicitly listed within this policy. Any queries relating to the applicable legislation should be directed to the policy author.

27. Equality and diversity

27.1 We will apply this policy consistently and fairly and will not discriminate against anyone based on any relevant characteristics, including those set out in the Equality Act 2010.

28. Review

28.1 All policies should be reviewed every 3 years as a minimum, or sooner if there is a specific legislative, regulatory, or service requirement or change in guidance, law or practice.

Policy author:	**Policy and Performance Manager**	
Policy owner:	**Head of Corporate Services**	
Adopted from SNG: y/n	**Yes**	
Review schedule (1, 2 or 3 years):	**3 years**	
Equality Impact Assessment (EIA)	**Date completed**	**September 2024**
	Initial or full EIA	**Initial**

Change Record

Date	Reviewed by (name and	Version	Summary of changes
September 2021	Lisa Rae, Governance and Compliance Manager	V2	Adapted from NH to suit SW9's requirement
September 2024	Zoe Christodoulou, Policy and Performance Manager	V3	3 yearly review