BUSH & CO

Data Protection/GDPR

POLICY DOCUMENT

V 1.1

Document ID	**Data Protection/GDPR Policy**
Sponsor	**Karen Burgin**
Author	**Karen Burgin**
Date	**April 2018**

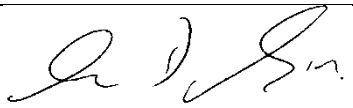
Version: 1.1

P:\Governance\Policies and Procedures\IT & Security

Version Control Log

Version	Date	Change
1.0	April 2018	New policy
1.1	September 2018	Review and amendments

Document Approval/Review

Name	Approval Signature	Approval Date	Next Review Due
Karen Burgin		April 2018	April 2019
Heather Ferguson		September 2018	April 2019

CONTENTS

1 OVERVIEW

General Data Protection Regulation 2018 ("the Regulation") applies to all organisations that handle personal data about living individuals including employees and customers ("personal data").

Bush & Co handles large amounts of personal data on a day-to-day basis and needs to ensure compliance with its obligations under the Act. This data includes personal sensitive data

The Data Protection Act 2018 (DPA) lays down eight key principles for the handling of personal data, and outlines certain conditions that must be satisfied before personal data can be processed. These conditions are even stricter if sensitive personal data is to be processed. The data Bush & Co hold about our clients falls within the definition of 'sensitive' personal data.

Bush & Co are joint data controller with its consultants as they are jointly responsible for the collection of personal data, deciding how it is processed, where stored and who shared with. As such the Company needs to work together with its consultants to ensure compliance and reduce business risk to all involved.

2 PURPOSE

The purpose of this policy is to assist staff and self employed consultants in understanding and meeting the requirements of the General Data Protection Regulation 2018 (GDPR); to look after personal data regarding clients, consultants and employees in a fair and lawful manner.

3 SCOPE

It is the responsibility of those listed below to ensure they adhere to the Data Protection Policies within Bush & Co;

- All employees at March House and self-employed consultants within their home environments.
- All visitors, including consultants and staff from other companies within the group using the "hot desk areas".

4 GDPR REGULATIONS

The General Data Protection Regulations 2018 build on the Data Protection Act 1998 which established a framework of rights and duties which were designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details. The legislation itself is complex and, in places, hard to understand and continues to evolve. However, it is underpinned by a set of six straightforward, common-sense principles. If you make sure you handle personal data in line with the spirit of those

principles, then you will go a long way towards ensuring that you comply with the letter of the law.

5 DEFINITIONS

Below is a set of common terms and definitions used in relation to the GDPR:

Personal data is information about an identifiable individual. This includes any information which has been anonymised, but where the individual could still be identified by other information that the employee can access. The information may be held electronically or in a manual filing system alphabetised by peoples' names.

Sensitive personal data is information regarding an individual's racial or ethnic origin; political opinions; religions or similar beliefs; trade union membership; physical/mental health or condition; sexual life; offences committed or alleged to have been committed; proceedings for any alleged or committed offence and the resulting disposal or court sentence.

A data controller is the person who has ultimate responsibility for any personal data and who determines the purposes for which personal data is to be processed.

A data processor is any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

The Information Commissioner's Office (ICO) is the UK's independent public body set up to protect personal information and enforce data protection law. The Information Commissioner has powers to investigate complaints; issue Notices on data controllers; enter and inspect premises and information; fine† for non-compliance.

Data protection principles are six rules which must be complied with whenever personal data is handled.

Processing covers almost any action that can be carried out with personal data, including receiving, recording, holding, changing, retrieving, disclosing, erasing and destroying.

Data Protection Officer (DPO) is appointed if you are a public authority or body, or if you carry out certain types of processing activities.

The DPO assists with monitoring internal compliance, informs and to advises on data protection obligations, manages identified risk through a Data Protection Impact Assessment (DPIA) and act as a contact point for data subjects and the supervisory authority (ICO).

6 DATA PROTECTION PRINCIPLES

The Regulation provides that personal data can (with very limited exceptions) be used only in accordance with six rules of good information handling ("the Principles"). These six Principles prescribe

- Guidelines on the personal data life-cycle (creation/acquisition, holding, processing, querying, amending, editing, disclosure or transfer to third parties, and destruction ('the life-cycle')
- The purpose for which personal data are gathered and held
- Enshrine rights for data subjects

Principles

1. Shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

This means that individuals who are the subject of any personal data ("data subjects") must be told what personal data will be collected and what will be done with it. Bush & Company provides this information through Privacy Notices at the point of first contact with data subjects or at the point of data collection.

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

This means personal data is only collected for the specific purposes which are notified to data subjects at the time it is collected.

Personal data should be reviewed periodically to check that they are accurate and up to date and to determine whether retention is still necessary. In any event, Consultants must not retain client's personal data once they have completed the assignment.

Adequate measures should be taken to safeguard data so as to prevent loss, destruction or unauthorized disclosure. The more sensitive the data, the greater the measures that need to be taken.

Consultants working from home should ensure separate secure log in facilities for Bush & Co assignments, keeping them separate to other family connections.

3. Shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

This means only the personal data which is necessary for the purposes of the Company's relationship with the data subject is requested and stored.

4. Shall be accurate and where necessary kept up to date

Records must be kept up to date in so much as it remains relevant for the purposes collected. Consultants must not retain client's personal data once they have completed the assignment.

5. Shall 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

Personal data should not be held for longer than is necessary. Bush & Co records management policies should be consulted for guidance on what is necessary for each kind of data. The Company Retention & Archiving Policy sets out document retention periods.

6. 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

The Company holds a great deal of personal data including sensitive data. This personal data is stored securely and is only accessible by authorised personnel. Personal data is only disclosed to third parties where appropriate in accordance with the Act.

Adequate measures should be taken to safeguard data so as to prevent loss, destruction or unauthorized disclosure. The more sensitive the data, the greater the measures that need to be taken.

Consultants working from home should ensure separate secure log in facilities for Bush & Co assignments, keeping them separate to other family connections.

7 INTERNATIONAL DATA TRANSFERS

Personal data shall not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Where the Company transfers personal data outside of the EEA then appropriate due diligence will be undertaken to ensure adequate security is in place to protect the personal data.

8 PRIVACY BY DESIGN

The Company will continually look at ways, particularly by reference to improving technology, of adapting its processes so that the risks to personal data privacy are minimised.

Changes to existing processes and systems will undergo Data Privacy Impact Assessment screening and where appropriate will be escalated to the Data Protection Officer for guidance

9 DISCLOSURE OF PERSONAL DATA

Employees and consultants of Bush & Co may not disclose any personal data about clients, unless they are clear that they have been given authority by Bush & Co management to do so. Moreover, employees and consultants must comply with the provisions of the company Collection of Personal Data, Consent and Confidentiality and Subject Access Request policies when disclosing personal data.

No employee or consultant may disclose personal data to the police or any other public authority unless that disclosure has been authorized by the Bush & Company Data Protection Officer or senior manager on duty, in consultation with the Safeguarding Officer.

10 DATA SUBJECT RIGHTS

The Company will only process personal data in accordance with the data subject's rights. These include:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Data subjects must be informed of their rights under GDPR in the form of privacy notices at first contact and prior to the collection and processing of any personal data.

11 COMPLIANCE WITH THE POLICY STATEMENT

Bush & Co is obliged to comply with the Regulation and requires all employees and consultants to ensure that all processing of personal data is conducted in accordance with the Principles and the other requirements of the Act. All staff and consultants shall ensure that they adhere to this Policy Statement and the Principles when processing personal data. Failure to do so shall constitute a disciplinary offence and for consultants may result in a suspension of work.

Consultants and staff are responsible for compliance with GDPR in their own operations. Consultants are classed as joint data controllers for the purpose of data protection and need to make themselves fully aware of the responsibilities in that regard. Support and guidance can be obtained from the Data Protection Officer (DPO) at dataprotection@bushco.co.uk.

Related policies which compliment this one are set out in Section 5 and staff and consultants should familiarise themselves with them. They are available on the Source or they may be requested via dataprotection@bushco.co.uk or their Operations Manager or Head of Expert Witness.

The Company has appointed the Head of Quality and Service Delivery as its Data Protection Officer ("DPO"), for the purpose of providing advice on the conditions necessary to achieve compliance. The DPO is also responsible for arranging annual

notifications to the Information Commissioner and for dealing with requests from individuals to have access to their data.

From time to time the DPO may delegate any or all responsibilities to another suitably qualified member of the Senior Management Team.

Any queries in relation to this document or data protection generally should be raised with the DPO or relevant line manager.

12 STAFF AND CONSULTANT RESPONSIBILITIES

All staff employed by Bush & Co and external consultants are expected to:

- Acquaint themselves with, and abide by, the Data Protection Principles set out in section 5 of this document
- Read and understand this policy document and confirm such by signing the declaration issued by HR at the foot of this document
- Understand how to conform to the standard expected at any stage in the life-cycle
- Understand how to conform to the standard expected in relation to safeguarding data subjects' rights (e.g. the right to inspect personal data) under the Act
- Understand what is meant by 'sensitive personal data', and know how to handle such data
- Contact the Data Protection Officer (DPO) if in any doubt about the application or interpretation of the GDPR or if a query or request for information is received under the GDPR , and not to jeopardise individuals' rights or risk a contravention of the Act
- Contact the Bush & Co Data Protection Officer immediately to report any incident/theft including those related to laptops, desktops, smart phones and tablets.
- Comply with security measures provided by Bush and Co to protect the data subject
- Undertake GDPR as a minimum to understand their joint responsibilities and actions required to protect their clients and customers.
- Undertake appropriate training to ensure they have the skills and understanding to undertake their role within GDPR.

13 RISKS

Failure to comply with the Principles may also have a number of detrimental effects on Bush & Co and consultants as joint data controllers: -

- Risks to the safety and security of customer data especially sensitive personal data;

- Risk of fraudulent activity by customers, employees or third parties;
- Breach of agreements with our partners which require us to process data in accordance with the Regulation;
- Inability to use the data obtained to its full potential;
- Damage to reputation leading to a loss of confidence in the services provided; and
- Potential censure, sanctions or fines from the Information Commissioner's Office or other regulatory body

14 GENERAL DATA PROTECTION GUIDANCE

14.1 Protect Information Held Electronically

- Always access and work on case documents using the Company "Matter Sphere" software package only. This ensures that data remains secure and is backed-up
- Only in the event that it is not possible to use the "Matter Sphere" software package, downloaded files may be stored on encrypted PCs or laptops. Files must be routinely updated to the "Matter Sphere" storage drive to ensure data is backed-up and retained securely. Files downloaded to PC and laptop drives must be deleted when the work on them has been completed and the file(s) updated on the centrally administered "Matter Sphere"
- Using access controls to restrict access to information, i.e. unique passwords at log-on
- Password protecting files saved on encrypted portable storage devices, e.g. USB memory sticks
- Do not share / divulge passwords
- Change of password every 60 days as per issued guidance
- All devices through which company / client personal data is processed / stored must be encrypted with Bush & Co approved encryption software[1]. These devices include personal computers, tablets and memory sticks
- Phones through which company / client personal data is accessed must be PIN / fingerprint protected
- Ensure your computer screen is locked if stepping away from your desk in the office environment
- Do not leave portable devices (e.g. laptops) unattended when outside of the office environment
- Keeping the minimum information on portable storage devices
- Regularly backing up documents

[1] Details of approved encryption software will be issued separately.

- Wiping computers and other electronic storage devices when they are no longer needed
- Do not upload any company and / or case related data to online / cloud storage facilities unless expressly authorised by the Bush & Co Data Protection Officer. Documents may be downloaded from recognised online storage facilities only.
- Follow all guidance on ICT security from our IT administrators

14.2 Protect Paper Records

- Be aware of and comply with the company Secure Desk Policy
- Lock away paper files when they are not in use and at the end of each working day.
- Sensitive data should not be held in paper form unless absolutely necessary.
- When using paper records, initial or case ID should only be used to avoid sensitive data being accidently exposed beyond data processors agreed through consent e.g. therapists
- Do not leave confidential waste sacks lying around
- Only transport minimum information away from the office.
- Bush and Co will archive any key historical documents for the case if required. However, all case related documents should be saved to MatterSphere. Bush and Co will not take responsibility for the disposal/shredding or duplicate saving of case documents from consultants.
- It is the responsibility of the consultant to manage and destroy case documents they have used for the purposes of their role e.g. scanned or photocopied records.
- If Bush and Co receives documents for archiving, they will be reviewed and may be sent back to the consultant to sort and detail the purposes for archiving.
- Bush and Co will not shred consultant documents. This is the responsibility of the consultant as joint data controller.

15 RELATED POLICIES

- Secure Desk Policy
- Collection of Personal Data, Consent & Confidentiality Policy
- Mobile Phone & Tablet Security Policy

- Breach Reporting Policy
- Data Retention & Archiving Policy
- Password Policy
- Safeguarding Policy
- Subject Access Request Policy

16 REFERENCES

https://ico.org.uk/

https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/general-data-protection-regulation-gdpr

https://ico.org.uk/for-organisations/health/

https://www.dacbeachcroft.com/es/gb/articles/2016/november/a-guide-to-general-data-protection-regulation-in-health-and-social-care/

https://www.gov.uk/government/collections/data-protection-act-2018

17 CONFIRMATION OF RECEIPT

To be signed and sent to HR

Please sign a copy of Confirmation of Receipt and return to HR to acknowledge you have read, understood, comply and have completed relevant training to ensure compliance with GDPR regulations.

I have read and understood this GDPR/Data Protection Policy document and undertake to preserve the security and confidentiality of any information which may be acquired by me in the course of my work for Bush & Co.

As Joint Data Controller with Bush & Co I understand my responsibilities related to data protection and the possible penalties for non compliance when handling this information and to observe the data protection principles as set out in the General Data Protection Regulations 2018.

Signed: *Date:*

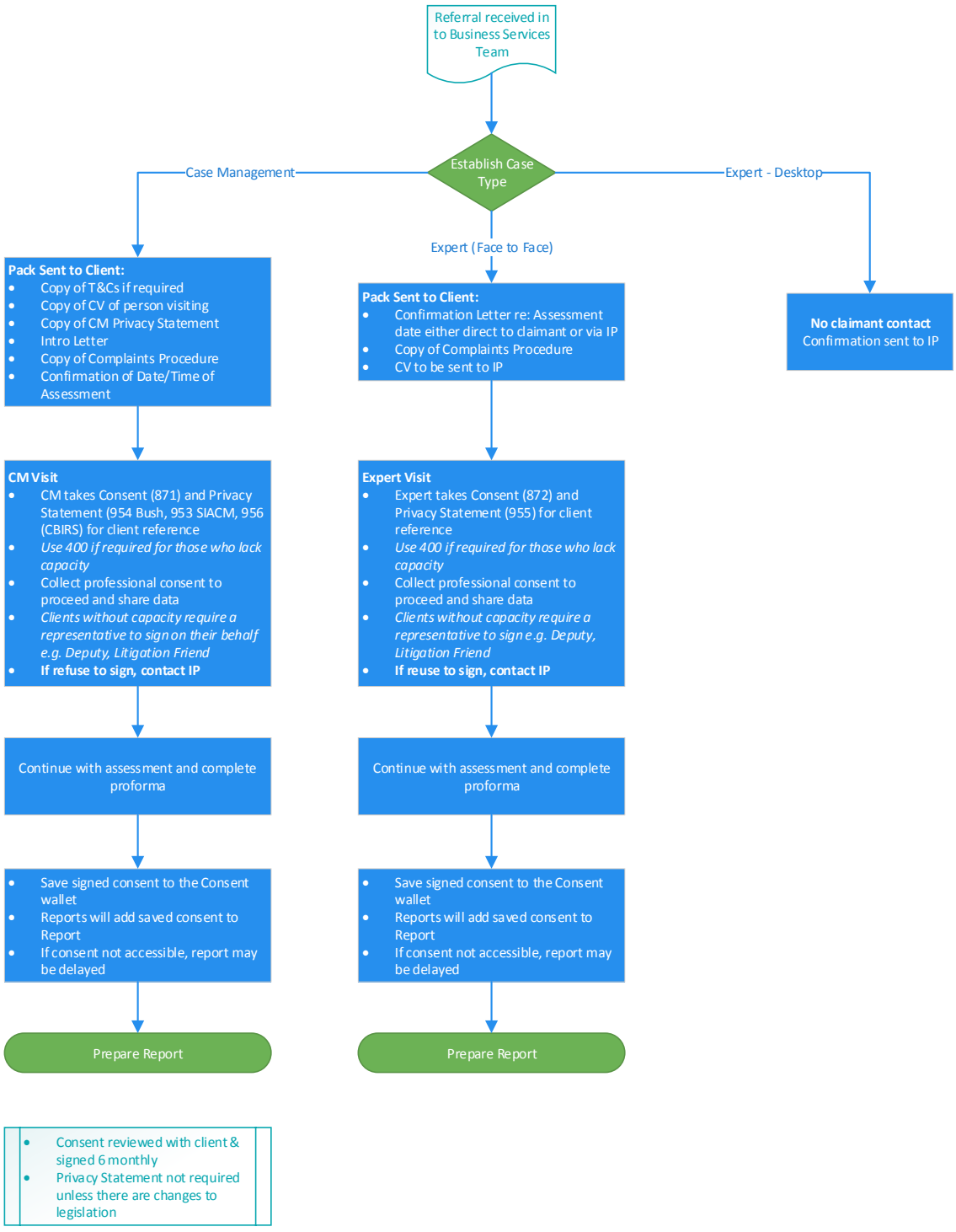
Name:

CM/EW:

Appendix 1

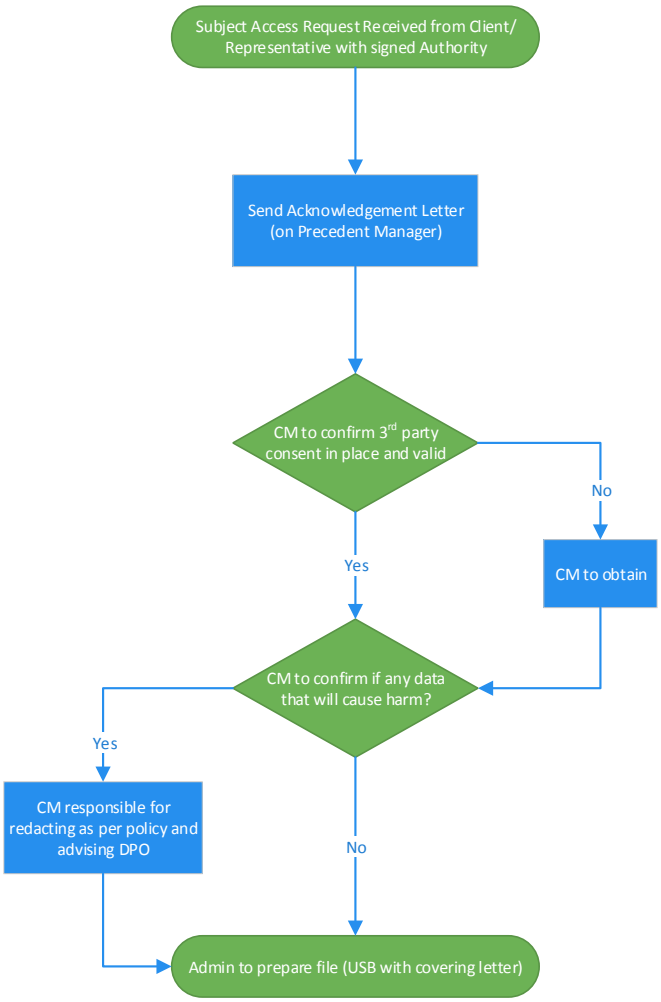
Procedure for Assessment re: Consent & GDPR

Version: 1
Date: 24/10/2018 **Owner: Heather Ferguson**



Appendix 2

Procedure for SAR for CM Records from Client/Representative (not Solicitor)
Version: 1
Date: 24/10/2018 **Owner: Heather Ferguson**

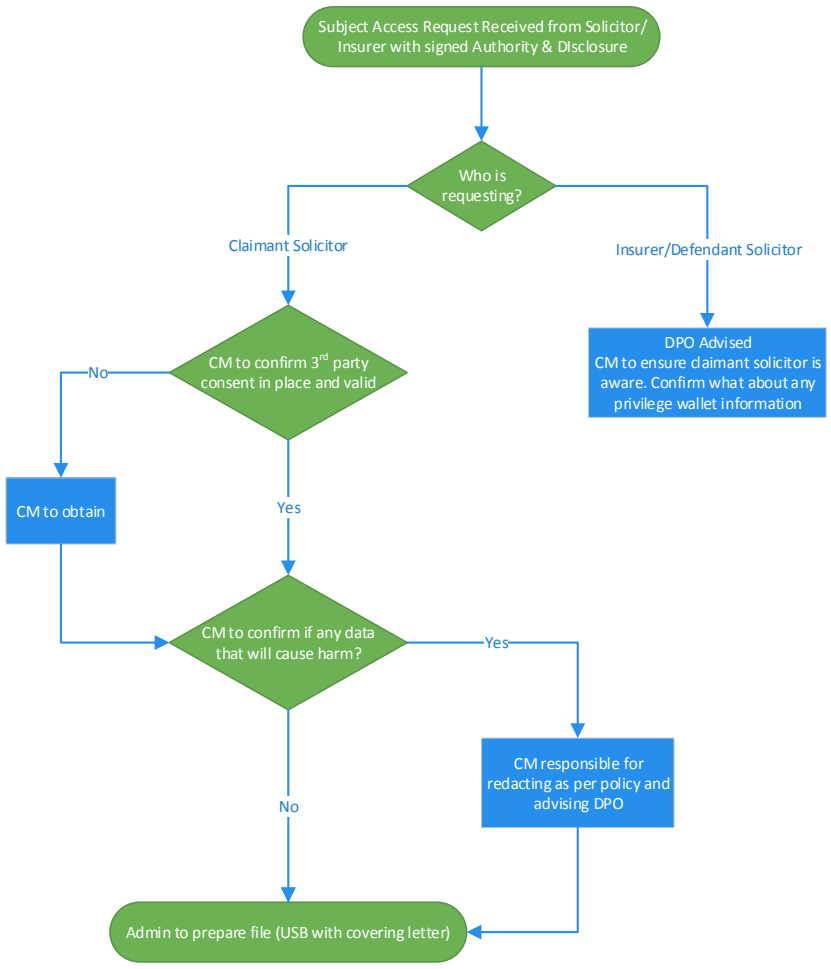


Appendix 3

Procedure for SAR for CM Records from Solicitor/Insurer

Version: 1

Date: 24/10/2018 **Owner: Heather Ferguson**



Within 30 days

Appendix 4

Procedure for SAR for Expert Record

Version: 1

Date: 24/10/2018 **Owner: Heather Ferguson**