**DATA PROTECTION LEGISLATIVE FRAMEWORK (GDPR)**

**Policy Statement**

The Data Protection Act 2018, which is based on the General Data Protection Regulation (GDPR) replaced the Data Protection Act 1998 in its entirety. It replaced the existing Data Protection Laws to make them fit for the digital age in which ever increasing personal data is being processed. The Act set new standards for protecting personal data, giving people more control over the use of their data and assists in the preparation for a future outside of the EU.

There are 4 main matters provided for, these are:

* General Data Processing
* Law Enforcement Data processing
* Data Processing for National Security Purposes
* Enforcement

All of the above need to be set in the context of international, national, and local data processing systems which are increasingly dependent upon internet usage for the exchange and transit of data. The UK must lock into international data protection arrangements, systems and processes and this Act updates and reinforces the mechanism to enable this to take place.

# Overview

The Act is structured in 7 parts, each of which covers specific areas. These are:

# 1: Preliminary

This sets out the parameters of the Act, gives an overview, explains that most processing of personal data is subject to the Act and gives the terms relating to the processing of personal data.

# 2: General Processing

This supplements the GDPR and sets out a broadly equivalent regime to certain types of processing to which the GDPR does not apply.

# 3: Law Enforcement Processing

This covers:

* “Competent authority”
* Meaning of “controller” and “processor”
* Data protection principles
* Safeguards concerning archiving and sensitive processing
* Rights and access of the data subject, including erasure
* Implements the law enforcement directive
* Controller and processor duties and obligations
* Records
* Co-operation with the ICO commissioner
* Personal data breaches
* The remedy of such breaches
* Position of the data protection officer and their tasks
* Transfer of data internationally to particular recipients
* National security considerations
* Special processing restrictions and reporting of infringements

# 4: Intelligence Services Processing

This covers only data handled by the above e.g. MI5 and MI6 and includes rights of access, automated decisions, rectification and erasure, obligations relating to security and data breaches.

# 5: The Information Commissioner

This covers

* General functions including publication of Codes of Practice and guidance
* Their International role
* Their responsibilities concerning specific Codes of Practice
* Consensual audits
* Information to be provided to the Commissioner
* Confidentiality and privileged communication
* Fees for services
* Charges payable to the commission
* Publications
* Notices from the Commissioner
* Reporting to parliament

# 6: Enforcement

This covers the new enforcement regime concerning all forms of Notice issued by the Commissioner.

* Powers of entry and inspection
* Penalty amounts
* Appeals
* Complaints
* Remedies in the court
* Offences
* Special purpose proceedings

# 7: Supplementary and Final Provision

This covers legal changes which the Act altered concerning other legal matters, e.g. Tribunal Procedure rules, definitions, changes to the Data Protection Convention etc. and List of Schedule(s).

As you can see, this Act is a huge piece of legislation, the majority of which is outside the remit of service providers working within the Adult Health and Social Care Sector. The I.C.O. confirms that many concepts and principles are much the same and businesses already complying with the current law are likely to be already meeting many of the key requirements of the GDPR and the Act.

The Information Commissioner says the Act represents a “step change” from previous laws. “It means a change of culture of the organisation. That is not an easy thing to do, and it’s certainly true that accountability cannot be bolted on: it needs to be a part of the organisations' overall systems approach to how it manages and processes personal data”. It is a change of mindset regarding data handling, collection, and retention.

We need to stop taking personal data for granted, it is not a commodity we own, it is only ever on loan. Individuals have been given control and we have been given the fiduciary duty of care over it!

As an organisation handling personal data on a day to day basis, this policy sets out the requirements of the Act and how we, as an organisation will meet our legal obligations. Staff awareness and understanding of their responsibilities regarding the handling, collection and retention of data will be core to the successful embedding of this policy.

**Preparation: (The 12 Steps)**

To comply with the requirements of the Act preparation should have included the completion of the 12 steps.

* Awareness
* Information we hold
* Communicating privacy information
* Individuals rights
* Subject access requests
* Lawful bases for processing
* Consent
* Children
* Data Breaches
* Data Protection by Design and Data Protection Impact Assessments
* Data Protection Officers
* International Data

# Definitions

The GDPR applies to “Controllers”, “Processors” and “Data Protection Officer” and to certain types of information, specifically, “Personal Data” and “Sensitive Personal Data” referred to in the Act as Special Categories of Personal Data”.

**“Controllers”** This role determines, on behalf of the organisation, the purposes and means of processing personal data.

**“Processors”** This role is responsible for processing personal data on behalf of a controller. The Act places specific legal obligations on you, e.g. you are required to keep and maintain records of personal data and processing activities. This role has legal liabilities if they are responsible for any breach.

**Data Protection Officer**

This role is a must only in certain circumstances if you are:

* A public authority (except for courts)
* Carry out large scale systematic monitoring of individuals e.g. online behaviour tracking, or
* Carry out large scale processing of special categories of data, or data relating to criminal convictions and offences e.g. Police, DBS Bodies, Prison Service etc. P33

 **“Personal Data”**

This means any information relating to an identifiable person can be directly or indirectly identified in particular by reference to an identifier. So, this would include name, reference or identification number, location data or online identifier. This reflects changes in technology that incorporates a wide range of different identifiers. Personal Data applies to both automated and manual filing systems. It can also apply to pseudonymised e.g. key-coded can fall within the GDPR dependent on how difficult it is to attribute the pseudonym to a particular individual. Race, ethnic origin, politics, religion, trade union membership, sex life or sexual orientation.

**“Special Categories of Personal Data”**

This category of data is more sensitive and much more protected. Sensitive personal data specifically includes genetic data, biometric data, health, race, ethnic origin, politics, religion, trade union membership, sexual orientation Safeguards apply to other types of data e.g. criminal convictions and offences or intelligence data etc.

# Data Protection Principles

The GDPR sets out the following principles for which organisations are responsible and must meet. These require that personal data shall be:

* Processed lawfully, fairly and in a transparent manner concerning individuals.
* Be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with purposes, further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes.
* Adequate, relevant, and limited to what is necessary for relation to the purposes for which they are processed.
* Accurate and where necessary kept up to date, every reasonable step must be taken that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.
* 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 may be stored for longer purposes in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the appropriate technical and organisational measures required by the GDPR (the safeguards) to safeguard the rights and freedoms of individuals; and
* Processed in a manner that ensures appropriate security of personal data. Including protection against unauthorised or unlawful processing and accidental loss. Destruction or damage, using appropriate technical or organisational measures.

“The controller shall be responsible for, and be able to demonstrate, compliance with the principles” Article 5 (2) GDPR

# “Lawful Bases” for Processing

There are 6 lawful bases for processing data. These are:

* **Consent:** the individual has given clear consent for us to process their personal data for a specific purpose.
* **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked us to take specific steps before entering into a contract.
* **Legal Obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).
* **Vital Interests:** the processing is necessary to protect someone’s life.
* **Public Task:** the processing is necessary for us to perform a task in the public interest, or for official functions and the task or function has a clear basis in law
* **Legitimate interests:** the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (Does not apply if a public authority is processing data to perform its official tasks).

# Consent

The GDPR sets a high standard here. Consent means offering individuals real choice and control. Consent practices and existing paperwork will need to be refreshed and meet specific requirements. These are:

* Positive opt-in, no pre-ticked boxes or other methods of “default” consent
* A clear and specific statement of consent
* Vague or blanket consent is not enough
* Keep consent requests separate from other terms and conditions
* Keep evidence of consent – who, when, how, and what you told people
* Keep consent under review
* Avoid making consent to processing pre-condition to any service
* Employers need to take extra care to evidence that consent is freely given, and should avoid over-reliance on consent

Consent is one lawful basis to consider but organisations in a position of power over individuals should consider alternative “lawful bases”. If we would still process their personal data without consent, then asking for consent is misleading and inherently unfair.

**PLEASE NOTE**

Consent within this policy relates only to data processing not Health or Support in a Social Care context. You must still use consent as defined within the Mental Capacity Act 2005 to deliver services

# Legal Obligation

Put simply, the processing is necessary for us as an organisation to comply with the law, e.g. the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014, which requires us as providers to collect, handle and process data in a prescribed manner.

**Legitimate Interests**

* This is the most flexible lawful basis for processing.
* It is likely to be appropriate where we process in ways that people would reasonably expect us to, with a minimal privacy impact, or where there is a compelling justification for the processing.

There are 3 elements to consider when using this lawful base. We need to:

* Identify a legitimate interest.
* Show that the processing is necessary to achieve it: and balance it against the individual’s interests, rights, and freedoms
* Legitimate interests can mean ours, the interest of third parties, commercial interests, individual or social benefits
* The processing must be necessary.
* A balance must be struck between our interests, the individual’s and would it be reasonable to expect the processing, or would it cause unnecessary harm, then their interests are likely to override our legitimate interests.
* Keep a record of your legitimate interest’s assessment (LIA) to help you demonstrate compliance.

The above are the 3 most pertinent bases for Health and Social Care data processing activity.

**Contract, Vital Interests or Public Task** apply within specific work settings and would be difficult to meet because service providers are subject to specific legislative and regulatory requirements to work within a “Regulated Activity”.

**“Lawful bases”** must be determined by the organisation before processing any personal data and thorough consideration must be given to this decision.

Service users or residents must be aware of the lawful base used by Zenith Care Recruitment to process their personal data.

**Individual Rights**

The GDPR provides the following rights for individuals:

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

Any individual request which falls into the above categories Zenith Care Recruitment will follow the relevant guidance currently available on the following website.

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/whats-new/>

# Privacy Notices, Transparency and Control

To start a privacy notice, you need to tell people, as a minimum

* Who you are?
* What you are going to do with their information
* Who it will be shared with?

Being transparent, and providing accessible information, is core to compliance and the GDPR. Privacy notices are the most common way to meet the GDPR requirements.

Transparency, in governance or business context, is honesty and openness and the more transparent we can be the more easily understood and accessible our services become to the people who use them. In the context of data processing is simply that

“It should be transparent to natural persons that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of their personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processor and further information to ensure fair and transparent processing in respect of the confirmation and communication of personal data concerning them which is being processed.”

**Information Commissioner: Role and Function**

The Information Commission Office is the UK’s supervising authority.

Within the Enforcement Toolbox, the Information Commissioners Office known as the I.C.O. can now issue substantial fines of up to 20 million, or, 4% of an organisation’s global turnover for certain data protection infringements. Fines, when appropriate, will be of the discretion of the I.C.O. with considerable variations expected to be levied. There are no fixed penalties or minimum fines, though there are different maximum fines for different breaches. The GDPR also empowers the I.C.O. to create tailor made solutions to deal with infringements brought to their attention. This does not mean that organisations can relax about compliance, but diligent small and medium sized organisations can take comfort in the fact that they are unlikely to face the sort of punitive fines that rogue tech giants could face.

Remember: the highest imposed fine limit was £500,000 under the old Act (1998) but the highest fine ever imposed was £400,000 to TalkTalk for failings in connection with a cyber-attack in 2016. The Information Commissioner is playing down the “scaremongering because of misconceptions”. £20 million fines could put businesses out of business and that is not the intention of the GDPR, though there is a seismic shift in the number of fines that could be imposed.

The role and scope of the I.C.O. has not fundamentally changed, but rather has been expanded and enhanced via the new GDPR.

**Codes of Conduct and Certification Mechanisms**

Although the use of any of the above is encouraged by the GDPR it is not obligatory. If an approved code of conduct or certification scheme becomes available that covers our processing activity, consideration will be given to working towards such a scheme as a way of demonstrating our compliance. The I.C.O. will develop its code of conduct as it has already worked with the Direct Marketing Commissions Code of Conduct: DMA Code.

**Derogations and Exceptions**

The Act provides that member states of the EU can provide their own national rules in respect of specific processing activities.

All Data Controllers must be familiar with Schedules 1-18 of the GDPR as these are the lawful exemptions pertinent to many other legal frameworks and Acts. These Schedules cover things such as Parliamentary Privilege, Health and Social Work, Criminal Convictions (Additional Safeguards), Research, Statistics and Archiving, Education Child Abuse, and include specific provisions for data processing within the Schedule(s).

**Codes of Practice**

The Act enhances the role of the Information Commission’s Office (I.C.O.) in the compilation of such Codes and these will be available in due course. We must be regularly checking the I.C.O. website to keep up with current guidance.

**Aim**

The aim of this policy is to instruct staff on the implications of data protection with regard to Zenith Care Recruitment.

This policy applies to all Zenith Care Recruitment employees and those acting on Zenith Care Recruitment’s behalf.

**The Policy**

Zenith Care Recruitment believes that all data, required for the delivery of the service and the lawful running of the organisation must be collected, handled, maintained, and stored following the requirements of the Data Protection Act 2018.

The General Data Protection Regulation (GDPR) form the basis of the Act but to be effective and compliant with its requirements, the Related Policy list should be viewed as core to this policy, as should Section 1 and the Related Guidance links.

Zenith Care Recruitment fully endorses and adheres to the principles of date protection, as enumerated in the Data Protection Act 1998.

Zenith Care Recruitment has responsibility to ensure that data subjects have appropriate access, upon written request, to personal information relating to them The policy sets out the over-arching guidance and principles that flow from the Data Protection Act 1998, the Caldicott Report recommendations, and the raft of other related legislation and central guidance which is used by organisations. The latter form of guidance will be used in this policy as ‘best practice’.

**Lawful Bases**

After due consideration, Zenith Care Recruitment has determined that the following Lawful Bases are used in the collection of data

* **[Contract:** the processing is necessary for a contract you have with the individual, or because they have asked us to take specific steps before entering into a contract.
* **Legal Obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).

Keeping Service users information physically and electronically secure

Zenith Care Recruitment Staff should not:

leave laptops, medical notes, rotas or files in unattended cars or in easily accessible areas. In the office all files and portable equipment should be stored under lock and key when not actually being used

Keeping Service User’ information secure: Office Staff

For using emails securely:

• Consider whether the content of the email should be encrypted or password protected. our IT or security team should be able to assist you with encryption.

• When we start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - eg “Dave” - the auto-complete function may bring up several “Daves”. Make sure you choose the right address before you click send.

• If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.

• Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.

• If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient’s arrangements are secure enough before sending your message.

For using faxes securely:

Consider whether sending the information by a means other than fax is more appropriate, such as using a courier service or secure email. Make sure you only send the information that is required. For example, if a solicitor asks you to forward a statement, send only the statement specifically asked for, not all statements available on the file.

· Make sure you double check the fax number you are using. It is best to dial from a directory of previously verified numbers.

· Check that you are sending a fax to a recipient with adequate security measures in place. For example, your fax should not be left uncollected in an open plan office.

· If the fax is sensitive, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine.

· Ring up or email to make sure the whole document has been received safely.

· Use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents.

For other security:

Shred all your confidential paper waste. Check the physical security of our premises.

Train our staff:

· so they know what is expected of them; to be wary of people who may try to trick them into giving out personal details;

· to use a strong password - these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols;

· not to send offensive emails about other people, their private lives or anything else that could bring your organisation into disrepute;

· not to believe emails that appear to come from your bank that ask for your account, credit card details or your password (a bank would never ask for this information in this way);

· not to open spam – not even to unsubscribe or ask for no more mailings. Tell them to delete the email and either get spam filters on your computers or use an email provider that offers this service

For all types of records, staff working in offices where records may be seen must:

· Shut/lock doors and cabinets as required.

· Wear building passes/ID if issued.

· Query the status of strangers.

· Know who to tell if anything suspicious or worrying is noted.

· Not tell unauthorised personnel how the security systems operate.

· Not breach security themselves.

Manual records must be:

· Formally booked out from their normal filing system.

· Tracked if transferred, with a note made or sent to the filing location of the transfer.

· Returned to the filing location as soon as possible after use.

· Stored securely within the office, arranged so that the record can be found easily if needed urgently.

· Stored closed when not in use so that contents are not seen accidentally.

· Inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorised persons.

With electronic records, Zenith Care Recruitment staff must:

· Always log-out of any computer system or application when work on it is finished.

· Not leave a terminal or mobile device unattended and logged-in.

· Not share logins with other people. If other staff have need to access records, then appropriate access should be organised for them – this must not be by using others’ access identities.

· Not reveal passwords to others.

· Change passwords at regular intervals to prevent anyone else using them.

· Avoid using short passwords, or using names or words that are known to be associated with them (e.g. children’s or pet’s names or birthdays).

· When transferring information by email to outside of the organisation all information should be password protected, the password should then be given separately from the original email

· It is advisable not to fax personal or confidential information.

Zenith Care Recruitment Field Based staff

For all types of records, staff working in the field where records may be seen must not:

· leave laptops, phones, tablets, medical notes, rotas or files in unattended cars or in easily accessible or viewable areas

· Staff should not normally take health care records home where this cannot be avoided, procedures for safeguarding the information effectively should be locally agreed

Rotas contain confidential information and the following is to be applied: -

* rotas or files are not to be left in unattended cars
* rotas are to be returned to the office for shredding
* All rotas if being emailed to workers should be password protected

Common Law and disclosure in the Public Interest

The key principle of the duty of confidence is that information confided should not be used or disclosed further in an identifiable form, except as originally understood by the confider, or with his or her subsequent permission.

There are exceptions to the duty of confidence that may make the use or disclosure of confidential information appropriate. Statute law requires or permits the disclosure of confidential Customer information in certain circumstances, and the Courts may also order disclosures. Case law has also established that confidentiality can be breached where there is an overriding public interest.

**Human Rights Act 1998**

Article 8 of the European Convention on Human Rights, which is given effect in UK law by the Human Rights Act, establishes a right to ‘respect for private and family life’.

This may be open to some interpretation in points of detail by the courts in years to come, but it creates a general requirement to protect the privacy of individuals and preserve the confidentiality of their health records. It underpins the Confidentiality Model presented in this code of practice. There are also more general requirements in relation to actions having legitimate aims and being proportionate to the need. Current understanding is that compliance with the Data Protection Act 1998 and the common law of confidentiality 26 should satisfy Human Rights requirements.

**DATA CONTROLLER – Kechinyere Anyanwu (kechia@zenithcarerecruitment.co.uk)**

# Individual Rights

There are several changes here in particular the Right of Access concerning timescales and fees. These must be fully understood concerning anyone submitting a Subject Access request. Please refer to the related Guidance Link.

The GDPR provides the following rights for individuals:

* Right to be informed
* Right of access
* Right to rectification
* Right to erasure
* Right to restrict processing
* Right to data portability
* Right to object
* Rights in relation to automated decision making and profiling.

Each of the above rights has its own Best Practice Process which you will find here.

<https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>

# Privacy Notices

This is a requirement for data processing, it is an accessible information declaration that should set out clearly how we will gather, use handle, store, and process personal data.

The Code uses the term “Privacy Notice” to describe all the privacy information that you make available or provide to individuals when you collect information about them. It is often argued that people’s expectations able personal data are changing, particularly through the use of social media, the use of mobile apps and the willingness of the public to share personal information via these platforms.

However, as an organisation, we are increasingly aware of the fragile trust which can be easily broken through data breaches and is therefore seeking transparency as a means of building trust and confidence with users of our services. It is the spirit of the Act that privacy, transparency, and control become a given for users.

Being transparent by providing a privacy notice is an important part of fair processing. When planning a privacy notice, we need to consider the following:

* What information is being collected?
* Who is collecting it?
* How is it collected?
* Why is it being collected?
* How will it be used?
* Who will it be shared with?
* What will be the effect of this on individuals concerned?
* Is the intended use likely to cause individuals to object or complain?

# Privacy and Electronic Communications Regulations (PECR)

This guide issued by the ICO covers specifically electronic marketing messages i.e. phone, fax, email, or text, and includes the use of cookies. It introduces specific roles on the above keeping such communication services secure and user’s privacy regarding traffic and location data, itemised billing, line identification and directory listings.

The Data Protection Act 2018 still applies if you are processing personal data. The PECR sets out some extra rules for electronic communications and please be mindful of electronic schedule systems which will also come under PECR.

**Data Protection By Design**

Zenith Care Recruitment has a general obligation to implement appropriate technical and organisational measures to demonstrate that we have considered the principles of data protection in our processing activities.

Any new systems of work or changes to our operational processes will involve consideration of how by default we as an organisation will have the necessary safeguards in place to prevent personal data from being made available without the consent of the person involved.

**Privacy Impact Assessment**

A Privacy Impact Assessment may be required when there is a large amount of data that is being collected and processed by the organisation.

A privacy Impact Assessment will include:

* Identification of data
* Evaluate the risks or breach
* Assess the Impact – the individual and organisation
* Devise Measures to mitigate risks
* Monitor review and update

The Data Controller is responsible for identifying when a Privacy Impact Assessment might be required.

**Reporting Breaches**

In the event where personal data has been breached the designated data lead or data controller must ensure that the Data Breach Plan is followed.

Breaches must be reported to the ICO within 72 hours of their discovery even if the nature of the breach is not yet fully known.

All persons affected by the breach should be notified as soon as possible after the breach has been identified. Support and advice should be provided where there is a risk present due to the breach

If there has been a deliberate breach by staff, then the company’s disciplinary processes will be invoked. Deliberate or malicious breaches could result in legal proceedings and prosecution.

# File Retention

The GDPR sets out Guidance on files and retention including archiving, specifically Health and Social Care personal data is generally exempt.

As a provider of services, file and retention guidelines are in place from our Regulator which includes CQC and the NHS as well as Local Authorities via the Service Specification within any contractual arrangements.

A periodic check of the Regulator’s Guidance should be part of the review of this policy.

# Compliance

To meet the requirements of the Act a thorough knowledge of the Guidance should be the priority for the Data Controller.

It is also important that the Act is placed in the context of other compliance requirements namely The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 and all other lawful requirements such as Regulation 18 Staffing to name but one.

In recognition of the complexities of the Act, the ICO has set up an advice service for small organisations.

**Related Policies**

* Adult Safeguarding
* Accessible Information and Communication
* Access to Records
* CCTV
* Confidentiality
* Consent
* Cyber Security
* Duty of Candour
* Record Keeping

**Training**

All Zenith Care Recruitment staffare made aware of the organisations' policies and procedures during induction, all of which are used for training updates. All policies and procedures are reviewed and amended where necessary and staff are made aware of any changes. Observations are undertaken to check skills and competencies. Various methods of training are used including one to one, online, group supervision, team meetings, individual supervisions.

Signed: \_\_\_\_\_\_\_Kechi A\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_15th November 2021\_\_\_\_\_\_\_\_\_\_\_\_

Policy review date: \_\_\_\_\_21st March 2022\_\_\_\_\_\_\_\_\_\_\_\_\_\_