wysdom®
dental technologies

GDPR
&
Data Protection

wysdom®
dental technologies

Wysdom GDPR Compliance

INTRODUCTION

This document explains how the Wysdom Practice Management Systems comply with the GDPR in respect of physical data protection and broader compliance.

Our own Data Protection Policies – also included in this document – outlines how we as a business are complying with GDPR in relation to our customers (Dental Practices) and in turn how their use of the Wysdom system impacts on their patients.

Our policies are relatively standard within the context of GDPR for our relationship with our customers as you will see; what all practices need to understand is that:

THE ABILITIES IN WYSDOM SOFTWARE ARE THERE TO HELP YOU COMPLY WITH YOUR OWN POLICIES AND IN PARTICULAR THE CONSENT ELEMENTS OF PATIENT RELATIONSHIPS. THEY ARE IN NO WAY YOUR GDPR COMPLIANCE - YOU MUST HAVE YOUR OWN POLICIES IN PLACE TO MEET GDPR.

As you already handle personal data you should already be registered with the ICO and working on your own policy compliance for GDPR. If you do not comply you are vulnerable as individuals and as a business.

See: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

GDPR - KEY FACTS

1. Personal Data as a definition, has become wider – so any information that can directly or indirectly identify a person is now considered as personal data.

2. Pre-ticked boxes are a big no-no and prospects must actively opt-in for ANY future marketing.

3. Individuals now have more rights:

- Right to be informed – Transparency is essential, every data subject must be made aware of their rights, the purpose and identify the lawful basis for processing the data.
- Right of access – You can no longer charge a fee should individuals ask for all their personal data (remember this applies to employees too)
- Right to rectification – You must rectify any incorrect data within 1 month (including 3rd parties)
- Right to erasure – Individuals have the right to be forgotten unless you have reasonable grounds to refuse this.
- Right to restrict processing – You must only retain the amount of personal data about the data subject that is necessary, so no further processing takes place
- Right to data portability – Where technically feasible, personal data should be sent directly to another data controller upon their request
- Right to object – You must cease processing immediately unless legitimate grounds can be demonstrated
- Rights with respect to automated decision-making and profiling – Data Subjects have the right to challenge such decisions, request human intervention and obtain an explanation from you.

4. All emails must be encrypted plus other data protection measures.

5. If you are transferring personal data to a country outside the EEA they must also comply.

6. All personal data must be secure and breaches must be reported within 72 hours to the ICO

7. The fines are huge for non-compliance:
€10 million (roughly £8 million) or 2% of your annual turnover whichever is higher – for not keeping proper records, violating data breach notification requirements and more
€20 million (roughly £16 million) or 4% of your annual turnover whichever is higher – for violating basic processing, ignoring individual's rights, incorrectly transferring personal data and more.

There are two primary aspects to address within the GDPR; security of data and protection of the rights of individuals.

Security of Data

Because of the highly sensitive nature of the data held on the Wysdom systems encrypt the whole Wysdom server disk(s), both locally and in the Cloud.

This means that besides using passwords to log into the server as a general user and then again as a Wysdom program user there may be a need for a Server Encryption Password or 2FA which you will need to process when you start or restart the machine.

Should a theft of the server or removal of disk(s) then occur the data stored, including all patient data in the

Wysdom system and any documents, reports etc., will not be accessible without the encryption password, rendering it useless in real terms.

Whilst standard Wysdom generated letters do not have personal data within them so do not need to comply, more general documents created outside Wysdom, like Word or Excel are not password protected in their own right so if a PC is left on and logged in, that could access unprotected data both locally and across a network to the server.

This means that you should log out and/or turn off computers when appropriate and never have any document or images data stored on local PCs or laptops – always keep everything on the server. Note though that this excludes some data held on X-Ray-specific PCs.

STORING DOCUMENTS. PLEASE NOTE THAT YOU SHOULD ONLY SAVE DOCUMENTS TO THE 'PRACTICE DOCUMENTS' FOLDER ON YOUR SERVER SO THEY ARE INCLUDED IN YOUR LOCAL AND CLOUD BACKUPS. IF YOU DON'T YOU COULD LOSE THEM WITH A DISK FAILURE.

See FAQs section for more details and best practice.

The Rights Of Individuals

GDPR demands that you only hold up-to-date data and you generally need the permission of patients to actually use their data.

There are field additions beings made to the patient record on (PC) screen and the patient tablet questionnaire to obtain permission for the transmission of patient data and how you may use data to contact patients.

These questions will need explicit opt-in by the patient and will be date-stamped in the patient notes; as will any changes made at a future date.

All data must be re-checked with the patient after three years, BUT best practice is to specifically ask about opt-ins every 12 months, so the Wysdom system will automatically highlight for this annually.

Tablet opt-in options will be included and recorded as part of the questionnaire completion.

Patient screen (on PC) options will need to be managed at the time of setting up new patients or for existing patients on their first visit after the GDPR update. Verbal consent to the different opt-in options is acceptable as long as it is documented. Note that the system will also register the operator that was logged in at the time of updating the patient opt-ins.

The "right to be forgotten" is a phrase used in GDPR and has been reported a lot in the press, giving the impression that anyone can demand to be entirely removed from any database should they choose but this is not the case in many circumstances – there are many exceptions listed in GDPR – so this is NOT an absolute right. Patients may therefore request that they be removed entirely from your system but the reality is that the practice has the right to retain their data because there are legitimate reasons to do so.

At the same time there is a right not to be contacted in the future so when you archive a patient their contact information will be removed entirely so a) a potential breach would not have that information and b) that they are not contacted by mistake. You can still 'un-archive' them if required at a future date.

Privacy statement

A standard privacy statement will be added to the footer of tablet forms referring to the practice's own policies. You should have copies of your policies available should they be asked for.

FAQs

- Where is the Cloud Backup data stored?

  All data is held in UK data centers.

- Is the Anti-Virus kept up to date?

  Industry standard Anti-Virus (AV) should be set up on all computers and automatically updated over the Internet.

  If you suspect the auto-updates are failing, you can check the status by opening up the AV. Click on the AV update status link.

- Are Wysdom-supplied laptops secure?

  Depending on the setup the system may use general network access OR a VPN (Virtual Private Network) connection so it is completely secure. BUT you should always log out or turn off when not using it.

- How secure are passwords?

  Data Protection is critical to GDPR and passwords are integral and vital to practice security. There is virtually no security if you use simple passwords or if you leave them written down.

  It is critical that all practices use STRONG, INDIVIDUAL passwords at all levels of access to your computers and programs. Use a minimum of 8 characters and include upper and lower case as well as numbers and symbols. Some experts recommend using three random words, but replace an "i" with a "1" perhaps or use a "5" instead of an "s". This all helps your security level.

  DO NOT:

1. **use generic passwords**
2. **share passwords**
3. **use the same passwords for computer access and Wysdom**

Do not leave passwords accessible or written down in unsecure places. For example, never leave a sticky (or any other) note on your screen or in your desk drawer.

There are software programs available to securely store passwords and phone apps are particularly useful for this as they also have their own security as another level.

If you want to strengthen Wysdom system passwords go to Utilities.

- How secure are Wysdom supplied practice computers?

  As explained earlier, Wysdom Servers will have an extra full encryption layer for all data, in case of theft.

  Servers, PCs and laptops should only be accessible by using strong passwords.

- When should computers be turned off?

  Servers should generally be left on because Cloud backups occur out of normal working hours.

  PCs should normally be turned off out of hours UNLESS INSTRUCTED BY WYSDOM SUPPORT because a machine is used for local backup. If you are not quite sure about a specific machine, ASK SUPPORT.

- What about X-Ray PCs?

  Generally, X-Ray PCs should be left on (logged-out) for backup purposes unless otherwise instructed by Wysdom support.

  NOTE: Some X-Ray program databases may not be encrypted (depending on the supplier and software version) and may be held locally on the X-Ray PC.

  To fully comply with GDPR and your own policies, where we have supplied your digital equipment or added it to your annual maintenance, Wysdom will install encryption level software on X-Ray PCs where appropriate to avoid data access should computer theft occur.

  If you have digital equipment not supplied or supported by us you should contact your supplier. If you have problems with them talk to us about supporting it – charges will apply.

- Are Servers, laptops and PCs vulnerable if left on?

  Yes, if you leave them logged in. So:

1. **when not in use, during working hours, all staff should log out or lock their computers, so programs and general files cannot be accessed by unauthorised staff, patients or visitors**

2. **at close of business always shut down your computers or close ALL programs and LOG OUT OF LEFT-ON COMPUTERS WHERE THERE IS A NEED TO ALLOW BACKUPS TO RUN**

SUMMARY

We have worked hard over the years to comply with GDPR as a business and to help you, our customers, in turn to comply with the legislation too. However, as so many areas are rather grey things may well change as case-law is established so we will endeavour to keep both us and our customers up to date.

But as we say earlier in this document, it's useless if you do not follow and enforce basic, common sense rules throughout your practice with regard to the accessibility of your computer system and the data you hold; we cannot do that for you.

After this section you will find our own Data Protection Policy – for reference.

If you have any thoughts or still unanswered questions just ask.

Wysdom Data Protection Plan

1. INTRODUCTION

This Policy sets out the obligations of Wysdom Dental Technologies Ltd, a company registered in Scotland under number SC114467, whose registered office is at Blue Square Virtual Offices, 272 Bath Street, Glasgow, United Kingdom, G2 4JR ("the Company/we/us/our") regarding data protection. It also sets out the way in which our Wysdom ICONic Software ("the Software") impacts on our clients.

This Policy sets out the rights of every individual ("data subject") whose personal data is collected, processed, transferred, stored, and disposed of, under the EU General Data Protection Regulation 2016/679 ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The procedures and principles set out in this Policy must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

We are committed not only to the letter of the law, but also to the spirit of the law and place high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom we deal.

2. THE DATA PROTECTION PRINCIPLES

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

a) Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
b) Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those 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.
c) Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
d) Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.
e) 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. Personal data may be stored for longer periods insofar 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 implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3. THE RIGHTS OF DATA SUBJECTS

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

a) The right to be informed (Part 14).
b) The right of access (Part 15);
c) The right to rectification (Part 16);
d) The right to erasure (also known as the 'right to be forgotten') (Part 17);
e) The right to restrict processing (Part 18);
f) The right to data portability (Part 19);
g) The right to object (Part 20); and
h) Rights with respect to automated decision-making and profiling (Parts 21 and 22).

4. OUR OBLIGATIONS IN RESPECT OF THE USE OF THE SOFTWARE

The Software is held on local servers by clients of ours and in the Cloud. We can gain remote access to the Software and the personal data contained therein for the purposes of updating and/or repairing the Software as necessary.

In addition, in the event of issues encountered with the Software or the system, clients may send the hard disk or server to us for investigation and where possible, repair. We may also, in that event, have access to the personal data.

We will comply with the provisions of this Policy when dealing with any personal data.

5. OUR CLIENTS' OBLIGATIONS IN RESPECT OF THE USE OF THE SOFTWARE

It is our clients' obligation to ensure any data subject whose data will be inputted to the Software has given their express consent for the processing of their personal data and has been informed of their rights under the GDPR, specifically that their personal data may be transferred to one or more third parties. This will enable us to comply with our obligations as specified in Part 4.

If the client sends their hard disk or server to us in accordance with Part 4, they must ensure this is transferred securely in accordance with Part 24.

Where the client requires us to provide hardware

manufactured by a third party, it is the client's obligation to obtain the third party's data protection policy to assess the hardware's suitability and establish we can comply with our obligations under this Policy.

6. LAWFUL, FAIR, AND TRANSPARENT DATA PROCESSING

The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

a) The data subject has given consent to the processing of their personal data for one or more specific purposes;
b) The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
c) The processing is necessary for compliance with a legal obligation to which the data controller is subject;
d) The processing is necessary to protect the vital interests of the data subject or of another natural person;
e) 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 the data controller; or
f) The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

7. SPECIFIED, EXPLICIT, AND LEGITIMATE PURPOSES

We collect and process the personal data set out in Part 23 of this Policy. This includes personal data collected directly from data subjects.

We only collect, process and hold personal data for the specific purposes set out in Part 23 of this Policy (or for other purposes expressly permitted by the GDPR).

The Software collects and processes the personal data set out in Part 23 of this Policy, only for the specific purposes set out in Part 23 of this Policy (or for other purposes expressly permitted by the GDPR). This includes personal data collected directly from data subjects.

Data subjects are kept informed at all times of the purpose or purposes for which we use their personal data. Please refer to Part 14 for more information on keeping data subjects informed.

8. ADEQUATE, RELEVANT, AND LIMITED DATA PROCESSING

We will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 7, above, and as set out in Part 23 below.

9. ACCURACY OF DATA AND KEEPING DATA UP-TO-DATE

We will ensure that all personal data collected, processed, and held by us is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 16, below.

The accuracy of personal data shall be checked when it is collected. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

10. DATA RETENTION

We will not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

Please ask for further information on our approach to data retention, including retention periods for specific personal data types.

11. SECURE PROCESSING

We will ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 24 to 29 of this Policy.

12. ACCOUNTABILITY AND RECORD-KEEPING

Our Data Protection Officer is Glenn Wynsor, who can be contacted at glenn@Wysdom.co.uk.

The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, any other data protection-related policies, and with the GDPR and other applicable data protection legislation.

We will keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a) Our name and details, our Data Protection Officer, and any applicable third-party data processors;
b) The purposes for which we collect, hold, and process personal data;
c) Details of the categories of personal data collected, held, and processed by us, and the categories of data subject to which that personal data relates;
d) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
e) Details of how long personal data will be retained by us; and
f) Detailed descriptions of all technical and organisational measures taken by us to ensure the security of personal data.

13. DATA PROTECTION IMPACT ASSESSMENTS

We will carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data.

Data Protection Impact Assessments shall be overseen by

the Data Protection Officers and shall address the following:

a) The type(s) of personal data that will be collected, held, and processed;
b) The purpose(s) for which personal data is to be used;
c) The objectives;
d) How personal data is to be used;
e) The parties (internal and/or external) who are to be consulted;
f) The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
g) Risks posed to data subjects;
h) Risks posed both within and to the Company; and
i) Proposed measures to minimise and handle identified risks.

14. KEEPING DATA SUBJECTS INFORMED

We will provide to any data subjects the information set out in this Part 14 at the time of collection of data to every data subject:

a) The business' details including, but not limited to, the identity of its Data Protection Officer;
b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 23 of this Policy) and the legal basis justifying that collection and processing;
c) Where applicable, the legitimate interests upon which we are justifying the collection and processing of the personal data;
d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
e) Where the personal data is to be transferred to one or more third parties, details of those parties;
f) Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 30 of this Policy for further details);
g) Details of data retention;
h) Details of the data subject's rights under the GDPR;
i) Details of the data subject's right to withdraw their consent to our processing of their personal data at any time;
j) Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);
k) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
l) Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

15. DATA SUBJECT ACCESS

Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which we hold about them, what it is doing with that personal data, and why.

Data subjects wishing to make a SAR should do by email to the Data Protection Officer at the email address specified in Part 12.

Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

All SARs received shall be handled by the relevant Data Protection Officer.

We will not charge a fee for the handling of normal SARs. We reserve the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

16. RECTIFICATION OF PERSONAL DATA

Data subjects have the right to require us to rectify any of their personal data that is inaccurate or incomplete.

The personal data in question will be rectified, and the data subject informed of that rectification, within one month of the data subject informing the relevant party of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

17. ERASURE OF PERSONAL DATA

Data subjects have the right to request that the personal data held about them is erased in the following circumstances:

a) It is no longer necessary for us to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
b) The data subject wishes to withdraw their consent to the holding and processing of their personal data;
c) The data subject objects to the holding and processing of their personal data (and there is no overriding legitimate interest to allow us to continue doing so) (see Part 20 of this Policy for further details concerning the right to object);
d) The personal data has been processed unlawfully;
e) The personal data needs to be erased in order for us to comply with a particular legal obligation.

We can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

a) to exercise the right of freedom of expression and information;
b) to comply with a legal obligation for the performance of a public interest task or exercise of official authority.

c) for public health purposes in the public interest;
d) archiving purposes in the public interest, scientific research historical research or statistical purposes; or
e) the exercise or defence of legal claims.

Therefore, the Software and our clients have the right to collect, use, retain and refuse to erase health data if the processing is necessary for the purposes of medical care, if the processing is necessary in the public interest for public health reasons, or if we can demonstrate that processing is necessary for scientific research purposes.

Unless there are reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

18. RESTRICTION OF PERSONAL DATA PROCESSING

Data subjects may request that we cease processing the personal data we hold about them. If a data subject makes such a request, we shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

19. DATA PORTABILITY

We may process personal data using automated means. Where data subjects have given their consent to the processing of their personal data in such a manner, or the processing is otherwise required for the performance of a contract between us and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

20. OBJECTIONS TO PERSONAL DATA PROCESSING

Data subjects have the right to object to the processing of their personal data based on legitimate interests and direct marketing (including profiling).

Where a data subject objects to the processing of their personal data based on its legitimate interests, such processing will cease immediately, unless it can be demonstrated that our legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

Where a data subject objects to the processing of their personal data for direct marketing purposes, we shall cease such processing immediately.

21. AUTOMATED DECISION-MAKING

We may use personal data in automated decision-making processes. Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge to such decisions under the GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision.

The right described in this Part 21 does not apply in the following circumstances:

a) The decision is necessary for the entry into, or performance of, a contract between us and the data subject;
b) The decision is authorised by law; or
c) The data subject has given their explicit consent.

22. PROFILING

We may use personal data for profiling purposes. When personal data is used for profiling purposes, the following shall apply:

a) Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;
b) Appropriate mathematical or statistical procedures shall be used;
c) Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and

All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 24 to 28 of this Policy for more details on data security).

23. PERSONAL DATA COLLECTED, HELD, AND PROCESSED BY THE COMPANY AND THE SOFTWARE

We collect, hold, and process personal data for the following purposes:

Type of Data	Data Held	Purpose of Data
Client Data	Name, address, email address, telephone number	To process orders from our clients, to inform them of new products or services available by way of direct marketing and to contact them for support purposes

The Software collects, holds, and processes personal data for the following purposes:

Type of Data	Data Held	Purpose of Data
Customer Data	Name, address, email address, telephone number, medical records	For the client to carry out their services
Customer Data	Name, address, email address and telephone number	For marketing purposes (including transferring to third parties under the terms of this Policy provided consent is given for this)

24. DATA SECURITY - TRANSFERRING PERSONAL DATA AND COMMUNICATIONS

The following measures will be taken with respect to all communications and other transfers involving personal data:

a) All emails containing personal data must be encrypted;
b) The Software is kept in an encrypted environment;
c) All emails containing personal data must be marked "confidential";
d) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
e) Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using normal post.

25. DATA SECURITY - STORAGE

The following measures will be taken with respect to the storage of personal data:

a) All electronic copies of personal data should be stored securely using passwords and data encryption;
b) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
c) All personal data stored electronically should be backed up regularly with backups stored offsite. All backups should be encrypted;
d) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to us or otherwise without the formal written approval of the Data Protection Officer and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and
e) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on our behalf where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating that all suitable technical and organisational measures have been taken).

26. DATA SECURITY - DISPOSAL

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

27. DATA SECURITY - USE OF PERSONAL DATA

The following measures will be taken with respect to the use of personal data:

a) No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on our behalf requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Protection Officer;
b) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on our behalf or not, without the authorisation of the Data Protection Officer;
c) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
d) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and
e) Where personal data held by us is used for marketing purposes, it shall be the responsibility of the relevant Data Protection Officer to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

28. DATA SECURITY - IT SECURITY

The following measures will be taken with respect to IT and information security:

a) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols;
b) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on our behalf, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords; and
c) All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. Any IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so.

29. ORGANISATIONAL MEASURES

The following measures will be taken with respect to the collection, holding, and processing of personal data:

a) All employees, agents, contractors, or other parties working on our behalf shall be made fully aware of both their individual responsibilities and our responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;
b) Only employees, agents, sub-contractors, or other parties that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data;
c) All employees, agents, contractors, or other parties handling personal data will be appropriately trained to do so;
d) All employees, agents, contractors, or other parties handling personal data will be appropriately supervised;
e) All employees, agents, contractors, or other parties handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
g) The performance of those employees, agents, contractors, or other parties handling personal data shall be regularly evaluated and reviewed;
h) All employees, agents, contractors, or other parties handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;
i) All agents, contractors, or other parties handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of ours arising out of this Policy and the GDPR; and
j) Where any agent, contractor or other party handling personal data fails in their obligations under this Policy that party shall indemnify and hold us harmless against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

30. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

The personal data will be held within the EEA. It will not be transferred to countries outside of the EEA.

31. DATA BREACH NOTIFICATION

All personal data breaches must be reported immediately to the relevant party's Data Protection Officer.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under the above paragraph) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned;
b) The categories and approximate number of personal data records concerned;
c) The name and contact details of the Data Protection Officer (or other contact point where more information can be obtained);
d) The likely consequences of the breach;
e) Details of the measures taken, or proposed to be taken, by us to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

32. IMPLEMENTATION OF POLICY

This Policy shall be deemed effective as of May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.