Terms and Conditions of Engagement.

Parties:

Owl Live Ltd, a company registered in England & Wales under company number 5202837 whose registered office is at Studio Seven, Skyhawk Avenue, Liverpool, L19 2QR And

(Company) a company registered in England under company number (Company no) whose registered office is at (Registered company address)
Date: XXXX

1. These Terms and Conditions along with the NDA (Non-disclosure agreement) and appendices, constitute an engagement for subcontracting which apply to all projects on an ongoing basis, as and when engaged. The signing and acceptance of these Terms and Conditions and NDA by the subcontractor do not in any way guarantee repeat or regular continuity of such business services to be provided.
2. The services to be provided for each project are to be strictly in accordance with the verbal briefing or briefing document provided by Owl Live Ltd, and such services are not to be changed or modified by the subcontractor by any reasons of quality, content, timing or sequencing, without the express agreement of Owl Live Ltd
3. All copyright and rights in the nature of copyright subsisting in any materials, including but not limited to quotations, estimates, briefing documents, designs, drawings and plans, that are specific to the project shall vest exclusively in Owl Live Ltd and the subcontractor hereby assigns to Owl Live Ltd the entire copyright and all other rights in the nature of copyright subsisting in any such materials
4. Any changes or modifications indicated or instructed directly by the Client, or other Suppliers and Subcontractors engaged, particularly but not limited to, onsite at an event for the project, are not to be undertaken or complied with unless expressly agreed to by Owl Live Ltd, and no liability will be accepted, financial or otherwise, for any unauthorised changes or modifications to the supply or contracted services. Such unauthorised changes or modifications may prejudice the contractual arrangements of Owl Live Ltd with the Client, for which the supplier or subcontractor will become liable.
5. All suppliers and subcontractors engaged are to co-operate with each other any project including during preparation dismantling and are to afford all reasonable opportunities to each other for carrying out their respective work and services, all to ensure a smooth and uninterrupted project programme.
6. All subcontractors are engaged on the strict understanding that they are under contract to Owl Live Ltd for their work and services for each project, being exclusive to Owl Live Ltd, and **any promotion otherwise is prohibited and breaches this contract arrangement with immediate termination thereof, furthermore this will be seen as a material breach of the NDA.**
7. All subcontractors are engaged on an exclusive basis to work on a particular project or with a particular client. It is considered a conflict of interest to work on the same project or with the same client in any capacity outside of Owl Live and therefore in breach of this agreement. Any potential conflicts of interest must be discussed prior to receiving any information about the client or project.
8. All subcontractors must strictly adhere to the standards stated in our IT, data protection and Information security policies at all times, a copy of which is attached to this document (Appendix A & B)
9. Payment terms: 30 days from date of invoice
10. Subcontractors are expected to carry appropriate insurances at all times and must provide Owl Live Ltd with a copy of all insurance documentation upon request
11. The supplier or subcontractor will be held liable for:
    a. Any occurrence during the project due to any failure by them to comply with the briefing and contracted services.
    b. Any act or omission of their servants, agents or employees, which causes harm to the project and/or Owl Live Ltd.
12. Should a problem occur, the subcontractor is responsible for notifying the Owl Live Ltd representative immediately in order to enable prompt remedying of any problem.
13. If any provision of the Terms and Conditions or any agreement is held by a court or competent authority to be invalid, illegal or unenforceable and can be deleted without altering the essence of these terms and conditions or the relevant agreement, the unlawful provision will be severed and the remaining provisions will remain valid and in full force and effect.
14. These terms and conditions are governed by and construed in accordance with English law and any dispute or question in connection with is subject to the jurisdiction of the English Courts.

Terms and Conditions of Engagement.

Non-Disclosure Agreement

1. The Parties are entering into commercial discussions, as a result of which it may become necessary or desirable for the Disclosing Party to disclose to the Receiving Party confidential information. The Parties understand that their relationship is one of mutual trust and confidence and wish to exchange such confidential information subject to the terms of this agreement.

2. Each party to this Agreement is referred to as 'the Recipient' when it receives or uses the Confidential Information disclosed by the other party.

3. The Recipient undertakes not to use the Confidential Information disclosed by the other party for any purpose except the Purpose, without first obtaining the written agreement of the other party.

4. The Recipient undertakes to keep the Confidential Information disclosed by the other party secure and not to disclose it to any third party [except to its employees and professional advisers] who need to know the same for the Purpose, who know they owe a duty of confidence to the other party and who are bound by obligations equivalent to those in clause 3 above and this clause 4.

5. The undertakings in clauses 3 and 4 above apply to all of the information disclosed by each of the parties to the other, regardless of the way or form in which it is disclosed or recorded but they do not apply to:

    a. any information which is or in future comes into the public domain (unless as a result of the breach of this Agreement); or

    b. any information which is already known to the Recipient and which was not subject to any obligation of confidence before it was disclosed to the Recipient by the other party.

6. Nothing in this Agreement will prevent the Recipient from making any disclosure of the Confidential Information required by law, however should such a request be made to the recipient, they must let the other party know with five (5) working days.

7. The Recipient will, on request from the other party, return all copies and records of the Confidential Information disclosed by the other party to the Recipient and will not retain any copies or records of the Confidential Information disclosed by the other party.

8. Neither this Agreement nor the supply of any information grants the Recipient any licence, interest or right in respect of any intellectual property rights of the other party except the right to copy the Confidential Information disclosed by the other party solely for the Purpose.

9. The undertakings in clauses 3 and 4 will continue in force indefinitely, subject to clause 5

10. This Agreement is governed by, and is to be construed in accordance with, English law. The English Courts will have non-exclusive jurisdiction to deal with any dispute which has arisen or may arise out of, or in connection with, this Agreement.

SIGNED: _____

PRINT: _____

TRADING AS:

ADDRESS:

Appendix A - Information Security Policy

Statement
The security and protection of information is fundamental to the effective and efficient working of the company and the maintenance of confidentiality. This policy provides a framework within which allows us to handle information and data in the most secure way, given the demands of the company.
Security is everyone's responsibility and all personnel working in and for the company must make every effort to comply with this policy.

Scope of policy

The need
To meet legal and professional requirements to our client, the company must use cost effective security measures to safeguard its information resources. This company security policy will ensure a consistent approach to the implementation of appropriate security controls against common threats.

The policy
The policy of the company is to accept willingly all obligations in respect of information security and to protect its information resources by implementing recognised best practice

Applicability
The policy shall apply to all partners and staff of the company and any other sub-contractors using the IT resources of the company.

Implementation
The requirements of the policy shall be implemented by all partners, staff and any other subcontractors. Any team member noting any area of conflict between this Policy and any other company Policy must bring it to the attention of the Holly Roberts - HR & Finance Manager as Security Officer of the company, immediately for conflict resolution. Holly Roberts will in any case be responsible for the routine periodic review of the Policy. Internal audit shall undertake independent reviews to assess the adequacy of implemented security measures including compliance with the Policy. Compliance with the Policy is the duty of all partners and staff. In serious cases, failure to comply with the Policy may be a disciplinary matter and could also result in a breach of the law or a criminal offence. Staff have an obligation to report suspected breaches of the Policy immediately to Holly Roberts in the case of a breach or suspected breach that could affect the security of Owl Live.

Information resources
The Policy applies to all information whether spoken, written, printed or computer-based, which is owned, held in the custody of, or used by the company.
The Policy also applies to all resources used in creating, processing, transmitting, storing, using or controlling that information.

Objectives of the policy

- The objectives of the Policy are to ensure that:
- Information is protected from unauthorised access, disclosure, modification or loss.
- Information is authentic.
- Information and equipment are protected from accidental or malicious damage.
- Security risks are properly identified, assessed, recorded and managed.
- Safeguards to reduce risks are implemented.
- Audit records on the use of information are created and maintained as necessary.
- All legal, regulatory and contractual requirements and standards of due care are met.

These objectives shall be achieved through the implementation of security controls as described in the remaining sections of this Policy.

Legal obligations
General
The company accepts its obligations to comply with the laws of the United Kingdom. All members of the team must be aware that there are legal requirements relating to information that must be met.
The principles of these are detailed below.

Data protection act

Terms and Conditions of Engagement.

Information held electronically that relates to individuals is subject to the Data Protection Act 1998, that places obligations on those who record and use personal data and the organisation for which the work.
Antony Greenberg – Managing Director (Holly Roberts deputising) is appointed Data Protection officer and is responsible for registration matters with the Office of the Data Protection Registrar, application of the Data Protection Principles and the briefing of all Data Users within the team.

Software copyright
Software is protected by the Copyright, Designs and Patents Act 1988, which state that 'the owner of the copyright has the exclusive right to copy the work'. It is illegal to make copies of software without the owner's permission. Penalties include unlimited fines and up to two year in prison.

Computer misuse act
The Computer Misuse Act 1990 established three prosecutable offences against unauthorised access to any software or data held on any computer. The offences are:

- Unauthorised Access to Computer Material
- Unauthorised Access with intent to commit or facilitate the commission of further offences
- Unauthorised Modification of Computer Material

Key security controls
Personal security
Holly Roberts and Antony Greenberg will ensure that all contracts of employment and any contracts of agency staff include a 'non-disclosure' clause. Holly Roberts will ensure that security responsibilities are allocated to staff and written into job specifications and terms of reference. Security education and training will be provided to all staff as appropriate to their assessed needs.

Physical security control
1. Principle
Resources associated with information processing, such as offices, computer equipment, communications media and paper-based records shall be protected from unauthorised access, misuse, damage or theft.
2. Access
The non-public areas of the company premises are designated a secure area. Visitors are to be escorted at all times and a record of visits kept.
3. Equipment Security
All hardware and software assets held by the company are to be held against a hardware register and be uniquely marked as being the property of the company. No alteration to the hardware configuration of the system may take place without the permission of Holly Roberts. On-going maintenance arrangements have been agreed with IT Answers (Company's IT Consultants). Only approved systems engineers and the relevant staff members will be allowed access to hardware or software and such access is recorded. No remote diagnosis or repair services are permitted unless they are through IT Answers or approved by Holly Roberts. All such diagnosis and repair is to be recorded.
The disposal of any storage media is subject to specific security control. Simple deletion of files is not adequate and the advice of IT Answers and Holly Roberts is to be sought before any disposal.

Internal security control
1. Principles
All information shall have an official owner who will be fully accountable for its protection and who will be responsible for:

- Assigning a security classification where appropriate.
- Defining who is authorised to access the information on a need-to-know basis.
- Assessing the risks to the security of the information and the impact of its loss, for both short and long periods.
- Employing suitable measures to reduce risks.
- Ensuring that equipment is only utilised for company business.
- Ensuring that information is authentic, correct, complete and auditable.
- Ensuring that information is backed up regularly and at a frequency commensurate with its usage.
- Safeguarding and retaining all company records.
- Ensuring that information exchange with external organisations within or without the NHS does not compromise the confidentiality of sensitive information, nor does it increase the risk of data corruption.

2. Security Incidents and Reporting
A security incident is defined as any event that could result or has resulted in:

- The disclosure of confidential information to any unauthorised individual.
- The integrity of the system or data being put at risk.
- The availability of the system or information being put at risk.

An adverse impact, for example:
- Embarrassment to the company, its clients or servants.
- Threat to personal safety or privacy.
- Legal obligation or penalty.
- Financial loss.
- Disruption of activities.

All incidents or information indicating a suspected or actual breach of security must be reported immediately to Holly Roberts. The types of incidents that can result in a breach of security are many and varied. Their severity will depend upon a myriad of factors but the majority will be innocent and unintentional and will not normally result in any form of disciplinary action. The likely result will be improved security and awareness throughout the company.

Any unusual incident must be reported to Holly Roberts who will maintain a record of incidents. If an incident is considered to be significant, Antony Greenberg is to be informed.
Any member of staff reporting a breach of security will have unhindered access to Holly Roberts. If that member believes the breach is as a result of an action or negligence on the part of Holly Roberts then the member will have access direct to Antony Greenberg

3. Virus Protection
A computer virus is a computer program, which 'infects' (modifies or attaches itself to) other computer programs. It then replicates itself and when a set of conditions arises it performs its intended function. This can range from a silly message to the destruction of the complete data holding of a system. A constantly running anti-virus software package has been provided and set to auto update latest virus signatures. This does not absolve users from specifically checking any externally sourced discs or emails for viruses before downloading any data or application.

4. Passwords
Passwords are an effective security measure only if they are properly constructed and kept secret. Partners and staff will follow the following routines for password management. All users should have an individual user name for logon. All passwords are to be changed on a regular basis through system forced password changes. Additionally, users are to change their password at any time that they feel their password has been compromised. Passwords should be given values that are not associated with personal characteristics, (e.g. children's names, telephone numbers, car registration numbers etc.) Simple and obvious strings of characters and numbers should not be used. It is recommended that a combination of alphabetic, numeric, upper and lower case and system characters be used. Passwords should not be written down except as possible reference by Holly Roberts under strict security control. Passwords are not to be revealed to or shared with other users, breach of this will be deemed as gross misconduct. System passwords are to be maintained in hard copy form by the Security Officer and held in a sealed envelope under secure arrangements.

5. System Access Controls
No terminal of PC is to be left logged on and unattended. Users leaving their workstation are to log off the system, or change user, to prevent unauthorised access.

6. Housekeeping
Data backup of the complete system will be effected daily by IT Answers. Users are responsible for the backup of data held on their PC hard disk, however all companies documents must be saved on the shared server to ensure minimum risk of lost data. All backup data will be accorded the same level of security as live data and held separately at an off-site secure location. Removable storage media such as DVDs, CDs, and USB sticks should be stored in a secure environment when not in use and have a secure password on all documents. Removable media use should be kept to a minimum and cleared after use. All software in use by the company must be licensed and networked applications may be subject to a limited number of users. Holly Roberts is to ensure that software is correctly used against licences held. Software is not to be loaded onto any system or PC without the express authority of Holly Roberts. This Policy is also to be reflected in employee's terms and conditions of employment.

7. Service Continuity Planning
Disaster Recovery and Service Continuity Contingency plans are to be produced to ensure the continued fulfilment of the company mission (please refer to continuity policy).

External security control

Terms and Conditions of Engagement.

1. General
Any person not directly a member of the company team is to be considered ‘external’.
2. Information Exchange
The exchange of information with, and between, other organisations shall take place within formal arrangements that reflect the legal requirements and the sensitivity of the information.

Role of the company security officer
Holly Roberts is the nominated Security Officer for the company and shall:
Under the direction of Antony Greenberg develop and manage the company security programme.

- Develop, issue and maintain the IT security strategy and Policy and agree them with Antony Greenberg
- Develop a strategic IT Disaster Recovery & Service Continuity Plan and advise the company on its implementation.
- Create an information security awareness programme to include whole company briefings, training and education.
- Provide information security consulting support to the company.
- Investigate breaches of security and report findings and recommended action to the company.
- Implement a compliance programme to evaluate the effectiveness of the information security programme.
- Report annually to Antony Greenberg on the effectiveness of the overall information security programme.

Policy review
This Policy is to be reviewed on an annual basis by Holly Roberts to take account of changing circumstances, legislation, technology and security risks. Any revisions to the Policy are to be approved by Antony Greenberg prior to implementation.

Appendix B - Data Protection Policy and Procedures

1. Data Controller

Owl Live Ltd is registered as a Data Controller under the terms of the Data Protection Act 1988. The registration number is Z1170261 and is due for renewal on 3rd April 2017. This covers all work carried out by employees of Owl Live Ltd. Data Protection enquiries should be made to the Data Protection Officer, Studio Seven, Dakota Business Park, Skyhawk Avenue, Liverpool, L19 2QR.

Antony Greenberg – Managing Director (Holly Roberts deputising) is appointed Data Protection officer and is responsible for registration matters with the Office of the Data Protection Registrar, application of the Data Protection Principles and the briefing of all Data Users within the team.

2. Principles of Data Protection as outlined in the Data Protection Act 1998

2.1 Anyone processing personal data must comply with the eight enforceable principles of good practice.

2.2 Data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subjects rights
- Secure
- Not transferred to countries outside of the EEC without adequate protection

3. Owl Live Commitment

Owl Live is committed to meeting its obligations under the Data Protection Act of 1998. Owl Live will strive to observe the law in all collection and processing of subject data and will meet any subject access request in compliance with the law. Owl Live will only use data in ways relevant to carrying out its legitimate purposes and functions in a way that is not prejudicial to the interests of individuals. Owl Live has adopted a Code of Practice for Sharing Personal Information which we will adhere to when sharing personal information between the Owl Live partners.

3.1 Employees of Owl Live will take due care in the collection and storage of any sensitive data and will do their utmost to keep all data accurate, timely and secure. Where notified of changes to personal data, Owl Live will amend records within 20 days of receipt of notification.

3.2 Owl Live Employees, whether permanent, or temporary, or sub-contractors, must be aware of the requirements of the Data Protection Act when they collect or handle data about an individual and appropriate training will be provided.

3.3 Owl Live Partners must not disclose data except within the Policy and Procedure on disclosures described in Paragraphs 10 and 11.

3.4 Data supplied to outside agencies must always be protected by a written contract.

3.5 All collection and processing must be carried out in good faith.

3.6 Owl Live will keep records of all complaints by data subjects and any subsequent follow up. Owl Live will also keep a record of all data access requests. There will be a repository of all Owl Live statements of Data Protection Law compliance and information about any contacts made with the Data Protection Registrar. This information will be available to staff and data subjects on request.

3.7 Owl Live will inform subjects of any processing, disclosure or transfer that does not fall within Owl Live's purpose in a way that any individual supplying could be expected to understand.

3.8 Owl Live will keep Data Protection notification up to date.

4. Policy on collecting subject data

Owl Live will only collect data that is relevant to the carrying out of the legitimate purposes and functions in a way that is not prejudicial to the interests of individuals. All data on individual subjects will be treated in a consistent way.

4.1 Subjects will be informed about how Owl Live will store and use the data at the time of collection. This will require a standard statement to be sent in all written requests for data and correspondence and a similar verbal script will be used for data collection by telephone.

4.2 Where Owl Live intends to use data for its main purposes, subjects will be deemed to have given their data for this purpose. If other use is to be made of the data, e.g. for the purpose of undertaking customer satisfaction surveys, they will be offered an opt-out for any mailings beyond this core purpose. Owl Live will honour this opt-out to the best of its ability.

4.3 Data may be collected by the use of a telephone monitoring system which is used to improve both staff training and the quality of the services offered by Owl Live.

4.4 Owl Live will strive to ensure that data collection is as accurate as is possible.

4.5 Data may be stored in many ways such as databases, manual files or Word or Excel files. The data will be collected consistently no matter where the data is to be stored.

Terms and Conditions of Engagement.

5. Sensitive Data
5.1 There are various categories of sensitive data relating to individuals. These include (a) racial or ethnic origin (b) physical or mental health (c) lifestyle, (d) sexuality (e) religious or cultural beliefs.
5.2 Owl Live undertakes not to collect sensitive data where it is unnecessary to do so to further Owl Live's purpose of providing effective communication and event management services.
5.3 Owl Live will strive to ensure that sensitive data is accurately identified and managed on collection.

6. Procedures for collecting subject data
6.1 Staff are responsible for ensuring that all personal and where appropriate sensitive personal data is collected accurately and fully. Staff are responsible for ensuring that sensitive data is identified when collected.
6.2 Staff will obtain permission from the subject that their data will be stored at the time of collection and transferred within the partner organisations providing the service only if necessary
6.3 All personal information should be dated at the time of collection so that records can be archived/anonymised at an appropriate time.

7. Data Protection Statements
7.1 When personal data, including personal sensitive data is collected by Owl Live, the following statement must be included in all written forms, letters and web/email communications:
7.2 Owl Live will store and process your data in accordance with the requirements of the Data Protection Act 1998. Owl Live will not provide your information to any organisations apart from Owl Live partners without your express permission
7.3 Emails transmitted by Owl Live will display the following statement:
'Disclaimer: Look, you probably won't read this disclaimer but it is important. Let me tell you why. It protects the privacy and information of the person for whom the email was intended. And if it was your information that someone else was reading, we're sure you'd want this protection. So if yours isn't the name on top, please delete the mail and notify us here at Owl Live - it would be much appreciated. Please note that copying, disseminating or taking any action based on the above information by anyone not intended as the recipient is unlawful. The views expressed in this message are those of the individual sender, unless specifically stated as those of Owl Live.

8. Policy for data storage and processing
8.1 Owl Live will only hold data that is relevant to the carrying out of its legitimate purposes and functions, in a way that is not prejudicial to the interests of individuals. Information will be accurate and timely and will be held in an environment as secure as possible. Owl Live Partners will be responsible for ensuring that all regular data care procedures are fully and conscientiously followed. All manual files and databases will be kept up to date and will be archived or destroyed from 2 years of the last contact (as determined by the nature of the data held. Where data is held in a paper format, procedures for the disposal of confidential waste will apply e.g. shredding.
8.2 Data no longer required for the legitimate purposes of Owl Live will be purged from computer systems from 2 years after the last contact.
All individual data will be kept secure, by regular office security procedures or through the controls over the computer network. Sensitive data will be treated with appropriate security.
8.3 Data processing within Owl Live, including data sharing by Owl Live partners will only take place in accordance with the Owl Live Code of Practice
8.4 Where data is passed to a third party for processing, Owl Live will ensure that a written contract is in place that states that the agent will work within Owl Live's data protection policy. Control of the data will not be allowed to move to the third party.

9. Procedure for data storing and processing
9.1 All staff must take responsibility for following through any data care work required of them to maintain accurate data systems. They are also responsible for any records they keep in any filing systems.
9.2. Archiving policies for data no longer needed in our storage systems will be set up for all data stores. A clear justification must be supplied for personal data to be kept beyond two years.

10. Security
10.1 All paper files containing personal data will be stored in a secure location. We will take all possible steps to prevent unauthorised access to the offices where Owl Live data is kept and due care will be taken to ensure the security of data in lockable filing cabinets. No documents containing personal data must be left on desks or in unlocked cabinets when not in use.
10.2 Any documents that contain personal data will be shredded.
10.3 All possible steps will be taken to maintain effective security for the whole of the computer system. Access to information stored on computer systems, including laptops should be appropriately password protected. employees will take all necessary steps to avoid careless loss of data, including when working remotely.

Terms and Conditions of Engagement.

11. Policy on disclosures
11.1 Owl Live will not allow personal and sensitive personal data collected from subjects to be disclosed to third parties except in circumstances which meet the requirements of the Data Protection Act. This will be where either the subject has consented to the disclosure, there is a serious risk of harm, where Owl Live receives information which may prevent a crime or assist in the detection of a crime, or where Owl Live is legally obliged to disclose the data.

12. Procedure on disclosures
12.1 Any general disclosure must be recorded and held by the Data Protection Officer and that each class of disclosure includes a clear justification as to why the disclosure is taking place.
12.2 Any new disclosure to be made must be checked for suitability with the Data Protection Officer beforehand who may refer to the Data Protection registrar for advice and guidance.
12.3 Any request for data based on a legal requirement, e.g. from Police or other body, must be put in writing and be checked by the Data protection Officer against the advice of the Data Protection Registrar before any data is disclosed.

13. Subject Access Policy
Owl Live will provide information in response to any reasonable subject access request and will ensure that data is kept in an accessible form to facilitate such subject access.

Procedure on subject access policy
13.1 Owl Live will make every effort to ensure that immediate action is taken when a data access request is received. The Data Protection Officer will be informed immediately.
13.2 A standard letter (amended as appropriate) will be sent to the subject stating Owl Live's policy on subject access. This will promise to provide an acknowledgement within 5 days and the required data to the best of Owl Live's ability within 20 days. Owl Live reserves the right to ask for a maximum payment of up to £10.
13.3 A search will be set up by the Data Protection Officer to ensure that all relevant data will be collected and collated ready to present to the subject. This will include all relevant electronic data and manual files. Information on data collection, storage, processing and transfer may also be required and statements will be prepared in advance. All relevant information will be prepared ahead.
13.4 The relevant information will be sent by secure email or registered post

14. Policy on complaints and queries
14.1 Owl Live will respond to any complaints as quickly as possible. Any letter or contact we receive in relation to the Data Protection Act, that questions our policy and/or procedure will be acknowledged within 5 working days, and responded to in full within 25 working days.
14.2 The Data Protection Officer will be advised without delay, of any complaints or queries relating to Data Protection policy or issues (as in 14.1 above)
14.3 Records will be kept of all correspondence for 5 years.

15. Procedure on complaints and queries
15.1 Notify the Data Protection Officer of the receipt of the complaint / query.
15.2 Copy all relevant documentation to the Data Protection Officer.
15.3 The Data Protection Officer will maintain a record of actions taken by staff to resolve a complaint or query.
15.4 Advise the Data Protection Officer of any further correspondence and developments as they occur.
15.5 On completion, records must be kept for 5 years

This Data Protection Policy will be reviewed on a regular basis