DATA PROTECTION AND DATA SECURITY POLICY

Statement and purpose of policy

A. Nigel Frost (the **Employer**) is committed to ensuring that all personal data handled by us will be processed according to legally compliant standards of data protection and data security.

B. We confirm for the purposes of the data protection laws, that the Employer is a data controller of the personal data in connection with your employment. This means that we determine the purposes for which, and the manner in which, your personal data is processed.

C. The purpose of this policy is to help us achieve our data protection and data security aims by:

   1. notifying our staff of the types of personal information that we may hold about them, our customers, suppliers and other third parties and what we do with that information;
   2. setting out the rules on data protection and the legal conditions that must be satisfied when we collect, receive, handle, process, transfer and store personal data and ensuring staff understand our rules and the legal standards; and
   3. clarifying the responsibilities and duties of staff in respect of data protection and data security.

D. This is a statement of policy only and does not form part of your contract of employment. We may amend this policy at any time, in our absolute discretion.

E. For the purposes of this policy:

   1. **Data protection laws** means all applicable laws relating to the processing of Personal Data, including, for the period during which it is in force, the General Data Protection Regulation (Regulation (EU) 2016/679).
   2. **Data subject** means the individual to whom the personal data relates.
   3. **Personal data** means any information that relates to an individual who can be identified from that information.
   4. **Processing** means any use that is made of data, including collecting, storing, amending, disclosing, or destroying it.
   5. **Special categories of personal data** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

Data protection principles

1. Staff whose work involves using personal data relating to Staff or others must comply with this policy and with the following data protection principles which require that personal information is:

   a. **processed lawfully, fairly and in a transparent manner.** We must always have a lawful basis to process personal data, as set out in the data protection laws. Personal data may be processed as necessary to perform a contract with the data subject, to comply with a legal obligation which the data controller is the subject of, or for the legitimate interest of the data controller or the party to whom the data is disclosed. The data subject must be told who controls the information (us), the purpose(s) for which we are processing the information and to whom it may be disclosed.

Our legal bases for processing personal data for healthcare purposes, including appointment reminders, include public task or legitimate interests.

- When we provide services under the NHS General Optical Services contract (such as a sight test funded by the NHS), our legal basis for processing personal data in respect of that service is public task
- Otherwise our legal basis is legitimate interests

Our condition for processing special category data is the provision of health or social care.

We process our patients' personal data for marketing purposes with their consent or to meet a legitimate interest. This means we can tell you about eye care products and services that may be relevant to you. If you do not want us to process your personal data for marketing purposes, please let us know and we will stop.

b. **collected only for specified, explicit and legitimate purposes.** Personal data must not be collected for one purpose and then used for another. If we want to change the way we use personal data, we must first tell the data subject.

c. **processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing.** We will only collect personal data to the extent required for the specific purpose notified to the data subject.

d. **accurate and the Employer takes all reasonable steps to ensure that information that is inaccurate is rectified or deleted without delay.** Checks to personal data will be made when collected and regular checks must be made afterwards. We will make reasonable efforts to rectify or erase inaccurate information.

e. **kept only for the period necessary for processing.** Information will not be kept longer than it is needed and we will take all reasonable steps to delete information when we no longer need it. For guidance on how long particular information should be kept, contact the Data Protection Officer, or request a copy of our Data retention policy.

f. **secure, and appropriate measures are adopted by the Employer to ensure as such.**

Who is responsible for data protection and data security?

2. Maintaining appropriate standards of data protection and data security is a collective task shared between us and you. This policy and the rules contained in it apply to all staff of the Employer, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants and contractors, casual or agency staff, trainees, homeworkers and fixed-term staff and any volunteers (**Staff**).
3. Questions about this policy, or requests for further information, should be directed to the Data Protection Officer.
4. All Staff have personal responsibility to ensure compliance with this policy, to handle all personal data consistently with the principles set out here and to ensure that measures are taken to protect the data security. Managers have special responsibility for leading by example and monitoring and enforcing compliance. The Data Protection Officer must be notified if this policy has not been followed, or if it is suspected this policy has not been followed, as soon as reasonably practicable.
5. Any breach of this policy will be taken seriously and may result in disciplinary action up to and including dismissal. Significant or deliberate breaches, such as accessing Staff or customer personal data without

authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

What personal data and activities are covered by this policy?

6. This policy covers personal data:
    a. which relates to a natural living individual who can be identified either from that information in isolation or by reading it together with other information we possess;
    b. is stored electronically or on paper in a filing system;
    c. in the form of statements of opinion as well as facts;
    d. which relates to Staff (present, past or future) or to any other individual whose personal data we handle or control;
    e. which we obtain, is provided to us, which we hold or store, organise, disclose or transfer, amend, retrieve, use, handle, process, transport or destroy.
7. This personal data is subject to the legal safeguards set out in the data protection laws.

What personal data do we process about Staff?

8. We collect personal data about you which:
    a. you provide or we gather before or during your employment or engagement with us;
    b. is provided by third parties, such as references or information from suppliers or another party that we do business with; or
    c. is in the public domain.
9. The types of personal data that we may collect, store and use about you include records relating to your:
    a. home address,contact details and contact details for your next of kin;
    b. recruitment (including your application form or curriculum vitae, references received and details of your qualifications);
    c. pay records, national insurance number and details of taxes and any employment benefits such as pension and health insurance (including details of any claims made);
    d. telephone, email, internet, fax or instant messenger use;
    e. performance and any disciplinary matters, grievances, complaints or concerns in which you are involved.

Sensitive personal data

10. We may from time to time need to process sensitive personal information (sometimes referred to as 'special categories of personal data').
11. We will only process sensitive personal information if:
    a. we have a lawful basis for doing so, eg it is necessary for the performance of the employment contract; and
    b. one of the following special conditions for processing personal information applies:

i. the data subject has given explicit consent.

ii. the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject.

iii. the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent.

iv. processing relates to personal data which are manifestly made public by the data subject.

v. the processing is necessary for the establishment, exercise, or defence or legal claims; or

vi. the processing is necessary for reasons of substantial public interest.

12. Before processing any sensitive personal information, Staff must notify the Data Protection Officer of the proposed processing, in order for the Data Protection Officer to assess whether the processing complies with the criteria noted above.

13. Sensitive personal information will not be processed until the assessment above has taken place and the individual has been properly informed of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

14. Our privacy notice sets out the type of sensitive personal information that we process, what it is used for and the lawful basis for the processing.

How we use your personal data

15. We will tell you the reasons for processing your personal data, how we use such information and the legal basis for processing in our privacy notice. We will not process Staff personal information for any other reason.

16. In general we will use information to carry out our business, to administer your employment or engagement and to deal with any problems or concerns you may have, including, but not limited to:

a. **Staff Address Lists:** to compile and circulate lists of home address and contact details, to contact you outside working hours.

b. **Sickness records:** to maintain a record of your sickness absence and copies of any doctor's notes or other documents supplied to us in connection with your health, to inform your colleagues and others that you are absent through sickness, as reasonably necessary to manage your absence, to deal with unacceptably high or suspicious sickness absence, to inform reviewers for appraisal purposes of your sickness absence level, to publish internally aggregated, anonymous details of sickness absence levels.

c. **Monitoring IT systems:** to monitor your use of e-mails, internet, telephone and fax, computer or other communications or IT resources.

d. **Disciplinary, grievance or legal matters:** in connection with any disciplinary, grievance, legal, regulatory or compliance matters or proceedings that may involve you.

e. **Performance Reviews:** to carry out performance reviews.

f. **Equal Opportunities Monitoring:** to conduct monitoring for equal opportunities purposes and to publish anonymised, aggregated information about the breakdown of the Employer's workforce.

Accuracy and relevance

17. We will:

a. ensure that any personal data processed is up to date, accurate, adequate, relevant and not excessive, given the purpose for which it was collected.

b. not process personal data obtained for one purpose for any other purpose, unless you agree to this or reasonably expect this.

18. If you consider that any information held about you is inaccurate or out of date, then you should tell the Data Protection Officer. If they agree that the information is inaccurate or out of date, then they will correct it promptly. If they do not agree with the correction, then they will note your comments.

Storage and retention

19. Personal data (and sensitive personal information) will be kept securely in accordance with our Information Security Policy.

20. We will usually keep any personal data we hold about you for ten years after our last contact with you before we delete it. This is the period recommended as good practice by the College of Optometrists. If we collected the data when you were aged under 18 we will keep it for ten years, or until your 25th birthday if that is later, in line with NHS requirements. In exceptional cases we may need to retain personal data for a longer period, and will explain our reasons for doing so on request.

.

Individual rights

20. You have legal rights in respect of the personal data we hold about you. The Information Commissioner's Office (ICO) has published guidance on the full range of rights. The rights that are most relevant to the way in which we use your personal data include:

21. Subject access requests:

a. You have the right to make a subject access request. If you make a subject access request, we will tell you:

i. whether or not your personal data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from you;

ii. to whom your personal data is or may be disclosed, including to recipients outside of the European Economic Area (EEA) and the safeguards that apply to such transfers;

iii. for how long your personal data is stored (or how that period is decided);

iv. your rights of rectification or erasure of data, or to restrict or object to processing;

v. your right to right to complain to the Information Commissioner if you think we have failed to comply with your data protection rights; and

vi. whether or not we carry out automated decision-making and the logic involved in any such decision making.

b. We will provide you with a copy of the personal data undergoing processing. This will normally be in electronic form if you have made a request electronically, unless you agree otherwise.

c. To make a subject access request, contact us at kevin@kingsbridgeeycare.co.uk.

d. We may need to ask for proof of identification before your request can be processed. We will let you know if we need to verify your identity and the documents we require.

e. We will normally respond to your request within 28 days from the date your request is received. In some cases, eg where there is a large amount of personal data being processed, we may respond within 3 months of the date your request is received. We will write to you within 28 days of receiving your original request if this is the case.

f. If your request is manifestly unfounded or excessive, we are not obliged to comply with it.

23. Other rights:

You have a number of other rights in relation to your personal data. You can require us to:

a. The right to be informed about how we use personal data – this privacy notice gives that information

b. The right to object – if you object to us processing your data for marketing purposes, or for healthcare purposes where our legal basis is legitimate interests (see 'why we collect and process your personal data', above), we will then stop doing so, unless we are processing the data in respect of a legal claim or can otherwise show that our legitimate interest in processing the data overrides your rights and interests

c. The right to rectification – if you ask us to correct personal data about you that is inaccurate or incomplete, we will do so within a month (unless we need longer, in which case we will discuss this with you)

d. The right to erasure – also known as the 'right to be forgotten'. If you ask us to delete your personal data, we will do so if there is no compelling reason to continue processing the data. However, this right does not apply to patient data that we process for healthcare purposes, such as patient records. We will not usually delete healthcare data before our usual time limit (see 'how we hold and share your personal data' above) where we have a duty to keep accurate records – for example, to comply with a legal obligation, or in connection with a legal claim. If you ask us to delete such data we will discuss this with you

- To request that we take any of these steps, please send the request to kevin@kingsbridgeeycare.co.uk.

Data security

24. We will use appropriate technical and organisational measures to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

25. Maintaining data security means making sure that:

a. only people who are authorised to use the information can access it;

b. where possible, personal data is pseudonymised or encrypted;

c. information is accurate and suitable for the purpose for which it is processed; and

d. authorised persons can access information if they need it for authorised purposes.

26. By law, we must use procedures and technology to secure personal information throughout the period that we hold or control it, from obtaining to destroying the information.

27. Personal information must not be transferred to any person to process (eg while performing services for us on or our behalf), unless that person has either agreed to comply with our data security procedures or we are satisfied that other adequate measures exist.

28. Security procedures include:

    a. Any desk or cupboard containing confidential information must be kept locked.

    b. Computers should be locked with a strong password that is changed regularly or shut down when they are left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others.

    c. Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used.

    d. The Data Protection Officer must approve of any cloud used to store data.

    e. Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.

    f. All servers containing sensitive personal data must be approved and protected by security software.

    g. Servers containing personal data must be kept in a secure location, away from general office space.

    h. Data should be regularly backed up in line with the Employer's back-up procedure.

29. Telephone Precautions. Particular care must be taken by Staff who deal with telephone enquiries to avoid inappropriate disclosures. In particular:

    a. the identity of any telephone caller must be verified before any personal information is disclosed;

    b. if the caller's identity cannot be verified satisfactorily then they should be asked to put their query in writing;

    c. do not allow callers to bully you into disclosing information. In case of any problems or uncertainty, contact the Data Protection Officer.

30. Methods of disposal. Copies of personal information, whether on paper or on any physical storage device, must be physically destroyed when they are no longer needed. Paper documents should be shredded and CDs or memory sticks or similar must be rendered permanently unreadable.

31. Additional measures to ensure data security include When sending emails to other health care professionals with personal data, the emails have to be encrypted. If there is a Data breach, a loss of a non-encrypted memory stick and/or a loss of data, you must inform the DPO (Kevin Frost) and/or the DPM (Danielle Clack). Both the DPO and DPM will liaise with the data protection team to resolve the issue within 30 days of it being raised. We have 30 days to notify the patients, should it be required..

Data impact assessments

32. Some of the processing that the Employer carries out may result in risks to privacy.

33. Where processing would result in a high risk to Staff rights and freedoms, the Employer will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches

34. If we discover that there has been a breach of Staff personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner within 72 hours of discovery.

35. We will record all data breaches regardless of their effect in accordance with our Breach response policy.

36. If the breach is likely to result in a high risk to your rights and freedoms, we will tell affected individuals that there has been a breach and provide them with more information about its likely consequences and the mitigation measures it has taken.

International data transfers

37. In the course of carrying out our business, we may need to transfer your personal information to a country outside the European Economic Area (EEA) including to any group company or to another person with whom we have a business relationship.

38. Your personal data will only be be transferred to a country outside of the EEA if there are adequate protections in place. To ensure that your personal data receives an adequate level of protection, we have put in place appropriate procedures with the third parties we share your personal data with to ensure your personal data is treated by those third parties in a way that is consistent with and which respects the law on data protection.

39. If you wish to know more about international transfers of your personal data, you may contact the Data Protection Officer.

Individual responsibilities

40. Staff are responsible for helping the Employer keep their personal data up to date.

41. Staff should let the Employer know if personal data provided to the Employer changes, eg if you move house or change your bank details.

42. You may have access to the personal data of other Staff members and of our customers in the course of your employment. Where this is the case, the Employer relies on Staff members to help meet its data protection obligations to Staff and to customers.

43. Individuals who have access to personal data are required:

    a. to access only personal data that they have authority to access and only for authorised purposes;

    b. not to disclose personal data except to individuals (whether inside or outside of the Employer) who have appropriate authorisation;

    c. to keep personal data secure (eg by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);

    d. not to remove personal data, or devices containing or that can be used to access personal data, from the Employer's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and

    e. not to store personal data on local drives or on personal devices that are used for work purposes.

Training

44. We will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

45. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy will receive additional training to help them understand their duties and how to comply with them.