Milton Keynes Dons

Data Protection Policy.

Author	John Cove
Role in Organisation	Director, Chair of MK Dons SET and Data Protection Officer
Date of Approval	February 2022
Date for Review	February 2024

Our Policy

Stadium MK Group is committed to complying with data protection law and to respecting the privacy rights of individuals. The policy applies to all of our staff, workers, directors, trustees, volunteers and consultants ("Workers").

This Data Protection Policy ("Policy") sets out our approach to data protection law and the principles that we will apply to our processing of personal data. The aim of this Policy is to ensure that we process personal data in accordance with the law and with the utmost care and respect.

This Policy applies to all companies in our Group of companies. References in this Policy to "us", "we", "ourselves" and "our" are to Stadium MK Group References to "you", "yourself" and "your" are to each employee / worker / volunteer to whom this Policy applies.

We recognise that you have an important role to play in achieving these aims. It is your responsibility, therefore, to familiarise yourself with this Policy and to apply and implement its requirements when processing any personal data.

Data protection law is a complex area. This Policy has been designed to ensure that you are aware of the legal requirements imposed on you and on us and to give you practical guidance on how to comply with them. This Policy also sets out the consequences of failing to comply with these legal requirements. However, this Policy is not an exhaustive statement of data protection law nor of our or your responsibilities in relation to data protection.

If at any time you have any queries on this Policy, your responsibilities or any aspect of data protection law, seek advice. Contact your line manager or John Cove, the Data Protection Officer (DPO).

This Policy is divided into two parts. Part 1 is to be read by all Workers. Part 2 is to be read by all Workers who work in the following fields: Directors; senior managers; human resources; finance; sales; security; data inputting, marketing;

information technology, coaching, teaching, performance and any other roles which involve the handling of personal data relating to individuals.

Part One | To be read by all workers

1. Who is responsible for Data Protection?

1.1 All our Workers are responsible for data protection, and each person has their role to play to make sure that we are compliant with data protection laws.

1.2 1.2We are required to appoint a Data Protection officer. Details of our current DPO can be found on the organisation's intranet and they can be reached at **data@stadiummk.com**

2. Why do we have a Data Protection policy?

2.1 We recognise that processing of individuals' personal data in a careful and respectful manner cultivates trusting relationships with those individuals and trust in our brand. We believe that such relationships will enable our organisation to work more effectively with and to provide a better service to those individuals.

2.2 This Policy works in conjunction with other policies implemented by us from time to time, including for example the Retention of Data Policy and any other policies we implement from time to time.

3. Status of this policy and the implications of breach?

3.1 Any breaches of this Policy will be viewed very seriously. All Workers must read this Policy carefully and make sure they are familiar with it. Breaching this Policy is a disciplinary offence and will be dealt with under our Disciplinary Procedure.

3.2 If you do not comply with data protection laws and/or this Policy, then you are encouraged to report this fact

3.3 immediately to our DPO. This self-reporting will be taken into account in assessing how to deal with any breach, including any non-compliance which may pre-date this Policy coming into force.

3.4 Also if you are aware of or believe that any other representative of ours is not complying with data protection laws and/or this Policy you should report it in confidence to our DPO. Our Whistleblowing Procedure will apply in these circumstances and you may choose to report any non-compliance or breach through our confidential whistleblowing reporting facility.

4. Other Consequences.

4.1 There are a number of serious consequences for both yourself and us if we do not comply with data protection laws. These include:

4.1.1 For you:

4.1.1.1. Disciplinary action: If you are an employee, your terms and conditions of employment require you to comply with our policies. Failure to do so could lead to disciplinary action including dismissal. Where you are a volunteer, failure to comply with our policies could lead to termination of your volunteering position with us.

4.1.1.2. Criminal sanctions: Serious breaches could potentially result in criminal liability.

4.1.1.3. Investigations and interviews: Your actions could be investigated and you could be interviewed in relation to any non-compliance.

4.1.2 For the organisation:

4.1.2.2. Civil Fines: These can be up to Euro 20 million or 4% of group turnover whichever is higher. These amounts are very substantial.

4.1.2.3. Assessments, investigations and enforcement action: We could be assessed or investigated by, and obliged to provide information to, the Information Commissioner on its processes and procedures and/or subject to the Information Commissioner's powers of entry, inspection and seizure causing disruption and embarrassment.

4.1.2.4. Court orders: These may require us to implement measures or take steps in relation to, or cease or refrain from, processing personal data.

4.1.2.5. Claims for compensation: Individuals may make claims for damage they have suffered as a result of our non-compliance.

4.1.2.6. Bad publicity: Assessments, investigations and enforcement action by, and complaints to, the Information Commissioner quickly become public knowledge and might damage our brand. Court proceedings are public knowledge.

4.1.2.7. Use of management time and resources: Dealing with assessments, investigations, enforcement action, complaints, claims, etc. takes time and effort and can involve considerable cost.

5. Data Protection Laws.

5.1 The Data Protection Act 1998 ("DPA") applies to any personal data that we process, and from 25th May 2018 this was replaced by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 ("DPA 2018") (together "data protection laws") and then after Brexit the UK will adopt laws equivalent to these data protection laws.

5.2 The data protection laws all require that the personal data is processed in accordance with the Data Protection Principles (on which see below) and gives individuals rights to access, correct and control how we use their personal data (on which see below).

6. Key words in relation to Data Protection.

6.1 The following are key terms that are commonly used in relation to data protection:

6.1.1 Personal data is data that relates to a living individual who can be identified from that data (or from that data and other information in or likely to come into our possession). That living individual might be an employee, member, coach, athlete, supplier, contractor or contact, and that personal data might be written, oral or visual (e.g. CCTV).

6.1.2 Identifiable means that the individual can be distinguished from a group of individuals (although the name of that individual need not be ascertainable). The data might identify an individual on its own (e.g. a name or video footage) or might do if taken together with other information available to or obtainable by us (e.g. a job title and company name). More details on this can be found in part 2 of this Policy.

6.1.3 Data subject is the living individual to whom the relevant personal data relates.

6.1.4 Processing is widely defined under the data protection laws and generally any action taken by us in respect of personal data will fall under the definition, including for example collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction of personal data, including CCTV images.

6.1.5 Data controller is the person who decides how personal data is used, for example we will always be a data controller in respect of personal data relating to our employees.

6.1.6 Data processor is a person who processes personal data on behalf of a data controller and only processes that personal data in accordance with instructions from the data controller, for example an outsourced payroll provider will be a data processor.

7. Outline.

7.1 The main themes of the data protection laws are:

7.1.1 good practices for handling personal data;

7.1.2 rights for individuals in respect of personal data that data controllers hold on them; and

7.1.3 being able to demonstrate compliance with data protection laws.

7.2 In summary, the data protection laws require us to:

7.2.1 only process personal data for certain purposes;

7.2.2 process personal data in accordance with the 6 principles of 'good information handling' (including keeping personal data secure, processing it fairly and in a transparent manner and keeping it for no longer than is required);

7.2.3 provide certain information to those individuals about whom we process personal data which is usually provided in a privacy notice, for example you will have received one of these from us as one of our staff;

7.2.4 respect the rights of those individuals about whom we process personal data (including providing them with access to the personal data we hold on them); and

7.2.5 keep adequate records of how data is processed and, where necessary, notify the regulator and possibly data subjects where there has been a data breach.

7.3 Every Worker has an important role to play in achieving these aims. It is your responsibility, therefore, to familiarise yourself with this Policy.

7.4 Data protection law in the UK is enforced by the Information Commissioner's Office ("ICO") and they are the regulator for data protection in the UK. The ICO has extensive powers, including the ability to impose civil fines of up to Euros 20 million or 4% of group worldwide turnover, whichever is higher. Also the data protection laws can be enforced in the courts and the courts have the power to award compensation to individuals.

8. Data Protection Principles.

8.1 The data protection laws set out 6 principles for maintaining and protecting personal data, which form the basis of the legislation. All personal data must be:

8.1.1 processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;

8.1.2 collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("purpose limitation");

8.1.3 adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("data minimisation");

8.1.4 accurate and where necessary kept up to date;

8.1.5 kept for no longer than is necessary for the purpose ("storage limitation");

8.1.6 processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("integrity and security").

8.2 More details on these principles can be found in Part 2 of this Policy.

9. Data Subject Rights.

9.1 Under data protection laws individuals have certain rights in relation to their own personal data. In summary these are:

9.1.1 The rights to access their personal data, usually referred to as a subject access request;

9.1.2 The right to have their personal data rectified;

9.1.3 The right to have their personal data erased, usually referred to as the right to be forgotten;

9.1.4 The right to restrict processing of their personal data;

9.1.5 The right to object to receiving direct marketing materials;

9.1.6 The right to portability of their personal data;

9.1.7 The right to object to processing of their personal data; and

9.1.8 The right to not be subject to a decision made solely by automated data processing.

9.2 Not all of these rights are absolute rights, some are qualified and some only apply in specific circumstances. More details on these rights can be found in Part 2 of this Policy.

10. Your Main Obligations.

10.1 What this all means for you can be summarised as follows:

10.1.1 Treat all personal data with respect;

10.1.2 Treat all personal data how you would want your own personal data to be treated;

10.1.3 Immediately notify your line manager or our DPOif any individual says or does anything which gives the appearance of them wanting to invoke any rights in relation to personal data relating to them;

10.1.4 Take care with all personal data and items containing personal data you handle or come across so that it stays secure and is only available to or accessed by authorised individuals; and

10.1.5 Immediately notify our DPO if you become aware of or suspect the loss of any personal data or any item containing personal data. [For more details on this see our separate Data Breach Policy which applies to all Workers regardless of their position or role in our organisation].

10.2 More detail on the obligations that apply to those staff who process personal data on our behalf can be found in Part 2 of this Policy which will apply to you if you are in a position or role which involves processing of personal data on behalf of our organisation.

11. Your Activities.

11.1 Data protection laws have different implications in different areas of our organisation and for different types of activity, and sometimes these effects can be unexpected.

11.2 Areas and activities particularly affected by data protection laws include Human Resources, payroll, security (e.g. CCTV), member/customer support, sales, [data inputting,] marketing and promotions, health and safety, finance, performance and participation

11.3 You must consider what personal data you might handle, consider carefully what data protection laws might mean for you and your activities, and ensure that you comply at all times with this policy.

12. Pratical Matters.

12.1 Whilst you should always apply a common sense approach to how you use and safeguard personal data, and treat personal data with care and respect, set out below are some examples of dos and don'ts:

12.1.1 Do not take personal data out of the organisation's premises (unless absolutely necessary).

12.1.2 Only disclose your unique logins and passwords for any of our IT systems to authorised personnel (e.g. IT) and not to anyone else.

12.1.3 Never leave any items containing personal data unattended in a public place, e.g. on a train, in a café, etc. and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.

12.1.4 Never leave any items containing personal data in unsecure locations, e.g. in car on your drive overnight and this would include paper files, mobile phone, laptops, tablets, memory sticks etc.

12.1.5 If you are staying at a hotel then utilise the room safe or the hotel staff to store items containing personal data when you do not need to have them with you.

12.1.6 Do encrypt laptops, mobile devices and removable storage devices containing personal data.

12.1.7 Do lock laptops, files, mobile devices and removable storage devices containing personal data away and out of sight when not in use.

12.1.8 Do password protect documents and databases containing personal data.

12.1.9 Never use removable storage media to store personal data unless the personal data on the media is encrypted.

12.1.10 When picking up printing from any shared printer always check to make sure you only have the printed matter that you expect, and no third party's printing appears in the printing.

12.1.11 Use confidential waste disposal for any papers containing personal data, do not place these into the ordinary waste, place them in a bin or skip etc., and either use a confidential waste service or have them shredded before placing them in the ordinary waste disposal.

12.1.12 Do dispose of any materials containing personal data securely, whether the materials are paper based or electronic.

12.1.13 When in a public place, e.g. a train or café, be careful as to who might be able to see the information on the screen of any device you are using when you have personal information on display. If necessary move location or change to a different task.

12.1.14 Do ensure that your screen faces away from prying eyes if you are processing personal data, even if you are working in the office. Personal data should only be accessed and seen by those who need to see it.

12.1.15 Do challenge unexpected visitors or employees accessing personal data.

12.1.16 Do not leave personal data lying around, store it securely.

12.1.17 When speaking on the phone in a public place, take care not to use the full names of individuals or other identifying information, as you do not know who may overhear the conversation. Instead use initials or just first names to preserve confidentiality.

12.1.18 If taking down details or instructions from a customer in a public place when third parties may overhear, try to limit the information which may identify that person to others who may overhear in a similar way to if you were speaking on the telephone.

12.1.19 Never act on instructions from someone unless you are absolutely sure of their identity and if you are unsure then take steps to determine their identity. This is particularly so where the instructions relate to information which may be sensitive or damaging if it got into the hands of a third party or where the instructions involve money, valuable goods or items or cannot easily be reversed.

12.1.20 Do not transfer personal data to any third party without prior written consent of your line manager or our DPO

12.1.21 Do notify your line manager or our DPO immediately of any suspected security breaches or loss of personal data.

12.1.22 If any personal data is lost, or any devices or materials containing any personal data are lost, report it immediately to our DPO [For more details on this see our separate Data Breach Policy which applies to all Workers regardless of their position or role in our organisation.

12.2 However you should always take a common sense approach, and if you see any areas of risk that you think are not addressed then please bring it to the attention of our DPO

13. Queries.

13.1 If you have any queries about this Policy please contact either your line manager or our DPO

13.2 There is also more detail on Data Protection contained in Part 2 of this Policy. Even if you are not required to read Part 2 of this Policy, you may find the answer to any queries you have in Part 2 and you are also encouraged to read Part 2.

Part Two | To be read by all Workers who work/volunteer in the following fields: Directors; senior managers; human resources; finance; sales; security; data inputting, marketing; information technology, coaching, teaching, performance and any other roles which involve the handling of personal data relating to individuals

14. Personal Data.

14.1 To expand on the information in Part 1 of this Policy data will relate to an individual and therefore be their personal data if it:

14.1.1 identifies the individual. For instance, names, addresses, telephone numbers and email addresses;

14.1.2 its content is about the individual personally. For instance, medical records, credit history, a recording of their actions, or contact details;

14.1.3 relates to property of the individual, for example their home, their car or other possessions;

14.1.4 it could be processed to learn, record or decide something about the individual (or this is a consequence of processing). For instance, if you are able to link the data to the individual to tell you something about them, this will relate to the individual (e.g. salary details for a post where there is only one named individual in that post, or a telephone bill for the occupier of a property where there is only one occupant);

14.1.5 is biographical in a significant sense, that is it does more than record the individual's connection with or involvement in a matter or event which has no personal connotations for them. For instance, if an individual's name appears on a list of attendees of an organisation meeting this may not relate to the individual and may be more likely to relate to the company they represent;

14.1.6 has the individual as its focus, that is the information relates to the individual personally rather than to some other person or a transaction or event he was involved in. For instance, if a work meeting is to discuss the individual's performance this is likely to relate to the individual;

14.1.7 affects the individual's privacy, whether in their personal, family, organisation or professional capacity, for instance, email address or location and work email addresses can also be personal data;

14.1.8 is an expression of opinion about the individual e.g. records stored in the course of a coaching assessment or details regarding a participant's performance; or

14.1.9 is an indication of our (or any other person's) intentions towards the individual (e.g. how a complaint by that individual will be dealt with).

14.2 Information about companies or other legal persons who are not living individuals is not personal data. However, information about directors, shareholders, officers and employees, and about sole traders or partners, is often personal data, so business related information can often be personal data.

14.3 Examples of information likely to constitute personal data:

14.3.1 Unique names;

14.3.2 Names together with email addresses or other contact details;

14.3.3 Job title and employer (if there is only one person in the position);

14.3.4 Video - and photographic images;

14.3.5 Information about individuals obtained as a result of Safeguarding checks;

14.3.6 Medical and disability information;

14.3.7 Member profile information (e.g. marketing preferences); and

14.3.8 Financial information and accounts (e.g. information about expenses and benefits entitlements, income and expenditure).

14.4 Examples of information unlikely to constitute personal data:

14.4.1 Reference to the individual's name in a document that contains no other personal data about that them (e.g. including the individual in a list of attendees of a meeting where the individual attended in an official capacity on behalf of a company); and

14.4.2 Where the individual's name appears in an email that has been sent to or copied to them, but where the content is not about him or her (e.g. emails sent to the individual about an organisation's dealings).

15. Lawful basis for Processing.

15.1 For personal data to be processed lawfully, we must be process it on one of the legal grounds set out in the data protection laws.

15.2 For the processing of ordinary personal data in our organisation these may include, among other things:

15.2.1 the data subject has given their consent to the processing;

15.2.2 the processing is necessary for the performance of a contract with the data subject;

15.2.3 the processing is necessary for the compliance with at legal obligation to which the data controller is subject; or

15.2.4 the processing is necessary for legitimate interest reasons of the data controller or a third party i.e. you are processing someone's personal data in ways they would reasonably expect it to be processed and which have a minimal privacy impact on the data subject or where there is a compelling justification for the processing.

16. Special Category Date.

16.1 Special category data under the data protection laws is personal data relating to an individual's race, political opinions, health, religious or other beliefs, trade union records, sex life, biometric data and genetic data.

16.2 Under data protection laws this type of information is known as special category data and criminal records history becomes its own special category which is treated for some parts the same as special category data. Previously these types of personal data were referred to as sensitive personal data and some people may continue to use this term.

16.3 To lawfully process special categories of personal data we must ensure that one of the following conditions has been met:

16.3.1 the individual has given their explicit consent to the processing;

16.3.2 the processing is necessary for the performance of our obligations under employment law;

16.3.3 the processing is necessary to protect the vital interests of the data subject. The ICO has previously indicated that this condition is unlikely to be met other than in a life or death or other extreme situation;

16.3.4 the processing relates to information manifestly made public by the data subject;

16.3.5 the processing is necessary for the purpose of establishing exercising or defending legal claims; or

16.3.6 the processing is necessary for the purpose of preventative or occupational medicine or for the assessment of the working capacity of the employee.

16.4 To lawfully process personal data relating to criminal records and history there are even more limited reasons, and we must either:

16.4.1 ensure that either the individual has given their explicit consent to the processing; or

16.4.2 ensure that our processing of those criminal records history is necessary under a legal requirement imposed upon us.

16.5 We would normally only expect to process special category personal data or criminal records history data usually in either:

16.5.1 Human Resources context and relating to posts that require a level of Criminal Record Check (CRC) and/or a Disclosure and Barring Service (DBS) check; and/or,

16.5.2 Where medical data is being held / processed

17. When do we process Personal Data?

17.1 Virtually anything we do with personal data is processing including collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction. So even just storage of personal data is a form of processing. We might process personal data using computers or manually by keeping paper records.

17.2 Examples of processing personal data might include (this is not an exhaustive list):

17.2.1 Using personal data to correspond with members;

17.2.2 Holding personal data in our databases or documents; and

17.2.3 Recording personal data in personnel or member files.

18. What does that mean?

18.1 We process personal data every day for any number of purposes and in any number of ways. We must, therefore, comply at all times with the Data Protection Principles.

19. Data Protection Principles and what you must do?

19.1 There are 6 data protection principles. You must comply with these principles when you process personal data.

19.2 There are indications in relation to each principle as to what you must and must not do. However, these are not exhaustive and for guidance only. You must use your common sense and be mindful of the potential implications to an individual of you processing their personal data. The principles are that personal data must be:

19.2.1 processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;

19.2.2 collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("purpose limitation");

19.2.3 adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("data minimisation");

19.2.4 accurate and where necessary kept up to date;

19.2.5 kept for no longer than is necessary for the purpose ("storage limitation"); and

19.2.6 processed in a manner that ensures appropriate security of the personal data using appropriate technical and organisational measures ("integrity and security").

20. Personal Data must be processed fairly, lawfully and transparently?

20.1 You must not process personal data obtained illegally (e.g. stolen). You must not process personal data obtained by misleading, pressurising or inducing an individual.

20.2 You must inform an individual: who the data controller is (i.e. Your manager) the purpose for which personal data is to be processed; and any additional information that is necessary to ensure that the processing is fair and transparent.

20.2.1 In the majority of cases, it will be sufficient for the individual to have been provided with our privacy notice applicable to the category of individual to satisfy this requirement. This can be done by using our approved standard forms, contracts and terms, and approved scripts, that contain our relevant privacy notices. Therefore, you must use approved standard documents and scripts at all times.

20.2.2 If you are processing personal data in a new or extraordinary way, you must confirm that this is covered by our privacy notice. If in doubt, seek advice from your line manager or the DPO.

21. Personal Data must be collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those purposes ("purpose limitiation").

21.1 You must only process personal data for purpose for which it was collected e.g. if you have taken a member's details to forward information to them on our products and services, you must not pass those details on to a third party seeking to promote their services.

21.2 If personal data is to be processed for another purpose, the individual must be informed of that purpose.

21.3 Again the purposes for which we collect and process personal data are set out in our standard privacy notices. This is another reason to make sure you always use our standard documents.

22. Personal Data must be adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("data minimisation").

22.1 You must ensure that the personal data can be used for the purposes for which it was collected. This means collecting what we need to collect, but not more personal data than we need nor too little personal data.

22.2 If we do not collect sufficient personal data to utilise it for its intended purpose, it should be securely deleted or destroyed.

22.3 If more personal data than is required has been collected, the unnecessary personal data should be securely deleted or destroyed.

22.4 When collecting personal data or recording personal data, think whether it is in fact needed for the purpose for which it is collected.

23. Personal Data must be accurate and, where necessary, keep up to date

23.1 When recording personal data make sure that you record it accurately. This is always important, but especially so where personal data is being entered into a database that may be reused on numerous occasions. Any mistakes or errors in the personal data will repeat themselves each time it is used.

23.2 Wherever possible, you must regularly confirm that personal data is correct and update databases accordingly (noting if personal data is incorrect and correcting it accordingly).

23.3 Where you become aware that personal data is incorrect, then the personal data should be corrected to remove the errors.

24. Personal Data must be processed in a manner that ensures appropriare security of the personal date using apporiate technical and organisational measures ("Intergrity and security").

24.1 You must delete data no longer required to fulfil the purposes for which it was originally collected.

24.2 Retention periods for data will be set out in our Data Retention Policy and also in our standard privacy notice provided to the individual.

24.3 What is 'necessary' will depend on the circumstances. Use your common sense and if in doubt, seek advice. Once deleted it may not be possible to retrieve personal data deleted in error so it is always best to check before permanently deleting any personal data.

24.4 Our systems are set up to automatically delete personal data where possible at the end of the relevant retention period.

25. Personal Data must be processed in a manner that ensures appropriare security of the personal date using apporiate technical and organisational measures ("Intergrity and security").

25.1 What are appropriate measures will depend on the circumstances, particularly the nature of the personal data you are processing, the harm that might result to the individual, the technologies available to you to keep personal data secure (e.g. encryption software) and the cost of measures.

25.2 Most of these technical and organisational measures are set for you by the organisation, and you just need to follow them. You must therefore follow all security policies, guidelines and instructions issued to you at all times. This includes both security for electronic systems and devices and also physical security.

25.3 Specific parts of the organisation will have responsibility for implementing various technical and organisational measures to protect personal data, for example IT in relation to our computer systems, and HR in relation to our Workers.

26. Foreign Transfers of Personal Data.

26.1 Personal data must not be transferred outside the European Economic Area (EEA) unless the destination country ensures an adequate level of protection for the rights of the data subject in relation to the processing of personal data or we put in place adequate protections.

26.2 These protections may come from special contracts we need to put in place with the recipient of the personal data, from them agreeing to be bound by specific data protection rules or due to the fact that the recipients own country's laws provide sufficient protection.

26.3 These restrictions also apply to transfers of personal data outside of the EEA even if the personal data is not being transferred outside of our group of companies.

26.4 You must not under any circumstances transfer any personal data outside of the EEA without your line manager's or our DPO's prior written consent.

26.5 We will also need to inform data subjects of any transfer of their personal data outside of the UK and may need to amend their privacy notice to take account of the transfer of data outside of the EEA.

26.6 If you are involved in any new processing of personal data which may involve transfer of personal data outside of the EEA, then please seek approval of your line manager or our DPO prior to implementing any processing of personal data which may have this effect.

27. Data Subject Rights.

27.1 Individuals have certain rights under data protection laws (Rights). These are:

27.1.1 the right of access (also known as a data subject access request)

27.1.2 the right to rectification

27.1.3 the right to erasure (also known as the right to be forgotten)

27.1.4 the right to restrict processing

27.1.5 the right to data portability

27.1.6 the right to object

27.1.7 rights in relation to automated decision making and profiling.

27.2 The exercise of these Rights may be made in writing, including email, and also verbally and should be responded to in writing by us (if we are the relevant data controller) without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. We must inform the individual of any such extension within one month of receipt of the request, together with the reasons for the delay.

27.3 Where the data subject makes the request by electronic form means, any information is to be provided by electronic means where possible, unless otherwise requested by the individual.

27.4 If we receive the request from a third party (e.g. a legal advisor), we must take steps to verify that the request was, in fact, instigated by the individual and that the third party is properly authorised to make the request. This will usually mean contacting the relevant individual directly to verify that the third party is properly authorised to make the request.

27.5 There are very specific exemptions or partial exemptions for some of these Rights and they will be discussed in relation to the specific right in sections 30 to 39 below.

27.6 Where an individual considers that we have not complied with their request e.g. exceeded the time period, they can seek a court order and compensation. If the court agrees with the individual, it will issue a Court Order, to make us comply. The Court can also award compensation.

27.7 The individual can also complain to the regulator for privacy legislation, which in our case will usually be the ICO, and they too can make us comply and can also impose a civil fine upon us.

27.8 In addition to the rights discussed in this document, any person may ask the ICO to assess whether it is likely that any processing of personal data has or is being carried out in compliance with the data protection laws. The ICO must investigate and may serve an information notice on us (if we are the relevant data controller) to obtain relevant information. The ICO may also conduct an informal investigation to start with, usually by writing a letter to us asking us to explain the position.

27.9 The result of any investigation may lead to an enforcement notice being issued by the ICO. Any letters, assessments, information notices or enforcement notices from the ICO should be immediately sent directly to our DPO.

28. Notification & Response Procedure.

28.1 If you receive a verbal request in relation to a Right, or believe you have a verbal request for the exercise of a Right, you should:

28.1.1 pass the call or person to your supervisor/manager if possible (unless you are a supervisor/manager). The supervisor/manager should make a written record of all relevant details and explain the procedure. If possible try to get the request confirmed in writing addressed to our DPO. If it is not possible to transfer the individual over then make a written record of the request and contact details for individual making the request; and

28.1.2 inform our DPO of the request and pass them any written records relating to the request.

28.2 If a letter or fax exercising a Right is received by you then you should:

28.2.1 pass the letter to your supervisor/manager;

28.2.2 the supervisor/manager must log the receipt of the letter with our DPO and send a copy of it to them; and

28.2.3 our DPO will then respond to the individual on our behalf.

28.3 If an email exercising a Right is received by you then you should:

28.3.1 pass the email to their supervisor/manager;

28.3.2 the supervisor/manager must log the receipt of the email with our DPO and send a copy of it to them; and

28.3.3 our DPO will then respond to the individual on our behalf.

28.4 Our DPO will co-ordinate our response which may include written material provided by our external legal advisors. The action taken will depend upon the nature of the request and the Right. Our DPO will write to the individual and explain the legal situation and whether we will comply with the request. A standard letter/email from our DPO should suffice in most cases.

28.5 Our DPO will inform the relevant management line of any action that must be taken to legally comply with any exercise of rights. Our DPO will also co-ordinate any additional activity required by our IT department to meet the exercise of any of the Rights.

28.6 The manager/senior manager who receives the request will be responsible for ensuring that the relevant response is made within the time period required.

28.7 Our DPO's reply will be validated by the relevant manager of the department producing the response. For more complex cases, the letter/email to be sent will be checked by our external legal advisors.

29. How to locate information for Data Subject Right requests and requests for the right to be forgotten.

29.1 If you are responsible for carrying out or co-ordinating any searches for personal data then this section will assist you in how you should approach carrying out the searches.

29.2 The personal data we need to provide in response to a subject access request, right to be forgotten or any other exercise of data subject rights may be located in several filing and/or network systems, so it is important to identify at the outset the type of information requested to enable a focused search.

29.3 However you should note that the individual is not obliged to clarify the scope of what we will need to search for, so whilst we can ask, we may not receive a useful clarification or any response at all. In this case we still have to comply with the original request.

29.4 Depending on the type of information requested, you may need to search all or some of the following:

29.4.1 electronic systems (e.g. databases, networked and non-networked computers, servers, customer records, human resources records system, email data, CCTV);

29.4.2 manual/paper filing systems (but only if they are 'structured filing systems', on which see below); and

29.4.3 any data systems held externally by our data processors.

29.5 If you are not authorised to access the relevant system or files that need to be searched, then you will not be able to carry out the search in those systems or files. In this case you will need to delegate those aspects of the search to a person who is authorised to access the relevant system or files.

29.6 You should conduct a reasonable search of the relevant systems using the individual's name, employee or membership number, address, national insurance number, telephone number, email address or other information specific to that individual. In each case the scope of the search may be different, and you should check with our DPO before commencing any search.

29.7 If information is not part of a structured filing system, it does not amount to personal data and will fall outside the scope of personal data under the data protection laws, and therefore will not be caught by the rights of data subjects.

29.8 To be a structured filing system, the system must be:

29.8.1 contain information relating in some way to individuals. Usually, there would be more than one file in the system or a group of information referenced by a common theme (e.g. an absence spread sheet). The files need not be located in the same geographical location, but could be dispersed over different locations;

29.8.2 structured by reference to individuals (e.g. by name or employee or account number) or by reference to information relating to individuals (e.g. type of job or location, address), so it is clear at the outset whether the system might contain information capable of amounting to personal data and, if so, in which file(s) it is held; and

29.8.3 structured so that specific information relating to a particular individual is readily accessible. This means that the system must be indexed or referenced so as to easily indicate whether and where in the file data about the individual is located.

29.9 Therefore, a structured filing system which is subject to the data protection laws must have an external and internal structure which allows personal data about an individual to be located relatively easily without having to conduct a manual search of the entire file. If you have to thumb through the whole file to find specific information, the file is not a structured filing system.

29.10 It might help to apply the 'temp test' to determine if a system is a relevant filing system. Ask yourself if a temp with no specialist knowledge of our internal processes and procedures could, if asked to retrieve information about a specified individual, identify that the system might hold such information and where in that system the information would be. If so it will be a structured filling system.

29.11 You should liaise with our DPO in relation to the searches to be carried out and they will also liaise with our IT department in relation to searches of our IT systems. Usually you will be required to carry out searches of any physical files or records.

30. Right of Access.

30.1 This paragraph contains the specific procedure to be followed where an individual exercises their right of access (also known as a data subject access request). The request need not refer to the Right, for instance, it might simply request 'a copy of all the information that you have about me'.

30.2 There are limited timescales within which we must respond to a request and any delay could result in our failing to meet those timescales, which could lead to enforcement action by the ICO and/or legal action by the affected individual.

30.3 The data protection laws gives individuals the right to obtain:

30.3.1 confirmation that their personal data is being processed;

30.3.2 access to their personal data; and

30.3.3 access to other supplementary information.

30.4 The individual is entitled to receive a description of the following:

30.4.1 the purposes for which we process the data;

30.4.2 the categories of personal data we process about them;

30.4.3 the recipients to whom we may disclose the data;

30.4.4 the duration for which the personal data may be stored;

30.4.5 the rights of the data subject under the data protection laws;

30.4.6 any information available regarding the source of the data were it is not collected from the data subject direct;

30.4.7 the right of the data subject to make a complaint to the supervisory authority for data protection;

30.4.8 the logic behind any automated decision we have taken about him or her (see below), the significance and consequences of this automated processing.

30.5 Plus we must also provide the information constituting the individual's personal data which is within the scope of their request. We must provide this information in an intelligible form and technical terms, abbreviations and codes must be explained, and where the request was made electronically we can, unless the data subject specifies otherwise, also provide the information in electronic form.

30.6 If the individual requests details on automatic decisions made about him, we must provide appropriate information, but in a format that does not compromise any trade secrets.

30.7 We may:

30.7.1 ask for additional information to confirm the identity of the individual making the request;

30.7.2 request that the scope of the request is narrowed in order to ease the searches to be undertaken (but the individual does not have to agree to such a request from us); and

30.7.3 where requests are manifestly unfounded or excessive, because they are repetitive: (a) charge a reasonable fee considering the administrative costs of providing the information (and the amount can be subject to limits); or (b) or refuse to respond. Where we refuse to respond to a request, we must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

30.8 Where we process a large quantity of information about an individual, the data protection laws permit us to ask the individual to specify the information the request relates to. The legislation does not introduce an exemption for requests that relate to large amounts of data, but we may be able to consider whether the request is manifestly unfounded or excessive.

30.9 We should verify the identity of the person making the request, using "reasonable means" if we are not sure about their identity.

31. Redactions.

31.1 Where we are providing information to an individual where they have made a subject access request, they are only entitled to their personal data. They are not entitled to see information which relates to other individuals or to other people, e.g. to a company.

31.2 In these cases we would redact, i.e. blank out in a permanent way, any information which is not the personal data of the individual making the subject access request.

32. Disclosing Personal Date to other individuals.

32.1 Sometimes information that is determined to be personal data about one individual might include information identifying or personal data about another person (e.g. an email between two people might contain personal information relating to both the sender and the recipient) and in some cases it is not possible to redact the information about the other person. There are additional steps to consider in relation to whether we disclose this information.

32.2 We must consider whether the other person has consented to the disclosure of their information or whether it would be reasonable to comply with the request without the other person's consent.

32.3 Where the other person has consented, their information can be disclosed.

32.4 Where the other person has not consented, whether it would be reasonable to disclose that person's information will depend upon all the circumstances and you must assess these on a case by case basis.

32.5 We would consider whether:

32.5.1 The other person has refused their consent;

32.5.2 The other person's consent cannot be obtained (e.g. because they are incapable of giving it due to illness or incapacity);

32.5.3 Asking for consent might reveal the identity of the individual making the request;

32.5.4 We owe the other person a duty of confidentiality;

32.5.5 We have taken any steps to obtain the consent of the other person;

32.5.6 The other person is a recipient or one of a class of recipients who might act on the data to the individual's disadvantage;

32.5.7 The other person is the source of the information;

32.5.8 The information is generally known by the individual; and

32.5.9 The individual has a legitimate interest in the disclosure of the other person's information which they have made known to us.

32.6 If you decide that the other person's information should be withheld (usually it should be), we still have to provide as much of the information requested as we can. Therefore, we should protect the other person's identity by redacting as much of this information and other identifiable particulars.

32.7 Always keep a record of what you have decided to do and your reasons for doing it.

33. Exemptions to the Right of Subject Access

33.1 In certain circumstances we might be exempt from providing personal data in response to a subject access request. These exemptions are described below and should only be applied on a case by case basis after a careful consideration of all the facts.

33.2 ***Crime detection and prevention***

33.2.1 We do not have to disclose personal data that we process for the purposes of preventing or detecting crime, apprehending or prosecuting offenders, or assessing or collecting any tax or duty, if and to the extent that giving subject access would be likely to prejudice any of these purposes.

33.3 ***Confidential references***

33.3.1 We do not have to disclose certain confidential references that we have given to third parties, but might have to disclose confidential references that we receive from third parties. Bear in mind that references received from third parties may contain personal data of another person, so you must consider the rules regarding disclosure of other party's personal data set out above.

33.4 ***Legal professional privilege***

33.4.1 We do not have to disclose any personal data that is legally privileged. The following would be legally privileged:

33.4.2 confidential communications between us and our lawyers where the dominant purpose of the communication is the giving or receiving of legal advice; and

33.4.3 confidential communications between us or our lawyers and a third party (e.g. a witness) where the dominant purpose of the communication is to give or seek legal advice in respect of current or potential legal proceedings. This claim to legal privilege would end as soon as the case has been decided and, at that moment, the documents in the file might be disclosable if a subject access request is received.

33.5 ***Management forecasting***

33.5.1 We do not have to disclose any personal data which we process for the purposes of management forecasting or management planning to assist us in the conduct of any organisation or any other activity (e.g. staff relocations, redundancies, succession planning, promotions and demotions) if and to the extent that disclosing the personal data would be likely to prejudice the conduct of that organisation or activity.

33.6 ***Negotiations***

33.6.1 We do not have to disclose any personal data consisting of records of our intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

33.6.2 In any cases of doubt then speak to our DPO and it may be that external legal advice is necessary in relation to whether or not an exemption can be applied in a particular case.

34. Right to Erasure.

34.1 The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of their personal data where there is no compelling reason for its continued processing.

34.2 The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have their personal data erased and to prevent processing in specific circumstances:

34.2.1 where their personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;

34.2.2 when the individual withdraws consent (but only to the extent that consent is the only basis for processing their personal data);

34.2.3 when the individual objects to the processing of their personal data and there is no overriding legitimate interest for continuing the processing;

34.2.4 where their personal data was unlawfully processed;

34.2.5 where their personal data has to be erased in order to comply with a legal obligation; and

34.2.6 where their personal data is processed in relation to the offer of information society services to a child.

34.3 There are some specific circumstances where the right to erasure does not apply and we can refuse to deal with a request:

34.3.1 to exercise the right of freedom of expression and information;

34.3.2 to comply with a legal obligation or for the performance of a public interest task or exercise of

34.3.3 official authority;

34.3.4 for public health purposes in the public interest;

34.3.5 archiving purposes in the public interest, scientific research historical research or statistical purposes; or

34.3.6 the exercise or defence of legal claims.

34.4 If we have disclosed the personal data to be erased to third parties, we must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

35. Right to Rectification.

35.1 An individual has the right to ask us to:

35.1.1 correct inaccurate personal data;

35.1.2 complete information if it is incomplete; and

35.1.3 delete personal data which is irrelevant or no long required for our purposes.

35.2 If we have disclosed the personal data in question to third parties, we must inform them of the rectification request where possible. We must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

35.3 If data is factually correct and we are justified in keeping it, i.e. it is relevant to the lawful purpose we are holding it for then we do not have to change or delete it, but the individual may make a request for erasure, i.e. the right to be forgotten, and in that case we would have to analyse the personal data and whether we can retain it based on that Right.

35.4 Where we are not taking any action in response to a request for rectification, we must explain why to the individual, informing them of their right to complain to the supervisory authority (usually the ICO) and to seek a remedy from the Courts.

36. Right to Restrict Processing.

36.1 An individual is entitled to require us to stop or not begin processing their personal data. When processing is restricted, we are permitted to store their personal data, but not further process it except in the exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest. We can retain just enough information about the individual to ensure that the restriction is respected in future.

36.2 We will be required to restrict the processing of personal data in the following circumstances:

36.2.1 where an individual contests the accuracy of the personal data, we should restrict the processing until we have verified the accuracy of the personal data;

36.2.2 where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our legitimate grounds override those of the individual;

36.2.3 when processing is unlawful and the individual opposes erasure and requests restriction instead; and

36.2.4 if we no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

36.3 Previously given consent for processing can be revoked at any time by the individual, therefore we cannot justify continued processing of data as a result of a previous consent.

36.4 The individual does not have this right if the individual has entered into a contract with us and the processing is necessary for the fulfilment of that contract.

36.5 We must inform individuals when we decide to lift a restriction on processing (for example, if an individual contested our right to process their personal data on legitimate interest grounds and we subsequently found that our processing was justified on these grounds).

36.6 If we have disclosed the restricted personal data to third parties, we must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

37. The Right to Data Portability.

37.1 The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. If the individual requests it, we may be required to transmit the data directly to another organisation if this is technically feasible. However, we are not required to adopt or maintain processing systems that are technically compatible with other organisations.

37.2 The right to data portability only applies:

37.2.1 to personal data an individual has provided to a data controller;

37.2.2 where the processing is based on the individual's consent or for the performance of a contract; and

37.2.3 when processing is carried out by automated means.

37.3 We must provide the personal data in a structured, commonly used and machine-readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data. The information must be provided free of charge.

37.4 If the personal data concerns more than one individual, we must consider whether providing the information would prejudice the rights of any other individual.

38. Right to Object.

38.1 Individuals have the right to object to:

38.1.1 processing based on legitimate interests;

38.1.2 the performance of a task in the public interest/exercise of official authority (including profiling);

38.1.3 direct marketing (including profiling); and

38.1.4 processing for purposes of scientific/historical research and statistics.

38.2 If we process personal data on the basis of our legitimate interests or the performance of a task in the public interest/exercise of official authority:

38.2.1 individuals must have an objection on "grounds relating to his or her particular situation"; and

38.2.2 we must stop processing the personal data unless we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims.

38.3 If we process personal data for direct marketing purposes:

38.3.1 we must stop processing personal data for direct marketing purposes as soon as we receive an objection. There are no exemptions or grounds to refuse;

38.3.2 we must deal with an objection to processing for direct marketing at any time and free of charge; and

38.3.3 we must nevertheless comply with the terms of the Privacy and Electronic Communication Regulations and the e-Privacy Regulation which replaces it.

38.4 If we process personal data for research purposes:

38.4.1 individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes; and

38.4.2 If we are conducting research where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing

38.5 If our processing activities fall into any of the above categories and are carried out online, we must offer a way for individuals to object online.

38.6 We must inform individuals of their right to object "at the point of first communication" and in our privacy notices. This right must be "explicitly brought to the attention of the data subject and is to be presented clearly and separately from any other information".

38.7

39. Automated Decision Making and Profiling.

39.1 The privacy legislation provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

39.2 We do not currently undertake any automated decision making. We must identify any of our subsequent processing operations that constitute automated decision making.

39.3 Individuals have the right not to be subject to a decision when:

39.3.1 it is based on automated processing; and

39.3.2 it produces a legal effect or a similarly significant effect on the individual.

39.4 We must ensure that individuals are able to:

39.4.1 obtain human intervention;

39.4.2 express their point of view; and

39.4.3 obtain an explanation of the decision and challenge it.

39.5 The right to obtain human intervention does not apply if the automated decision is

39.5.1 :necessary for entering into or performance of a contract between us and the individual;

39.5.2 authorised by law (e.g. for the purposes of fraud or tax evasion prevention); or

39.5.3 based on explicit consent (but bear in mind that any consent can be withdrawn).

39.6 The data protection laws define profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their:

39.6.1 performance at work;

39.6.2 economic situation;

39.6.3 health;

39.6.4 personal preferences;

39.6.5 reliability;

39.6.6 behaviour;

39.6.7 location; or

39.6.8 movements.

39.7 When processing personal data for profiling purposes, we must ensure that appropriate safeguards are in place. We must:

39.7.1 ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences;

39.7.2 use appropriate mathematical or statistical procedures for the profiling;

39.7.3 implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors; and

39.7.4 secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

39.8 Automated decisions taken for the purposes must not concern a child. Automated decisions must not involve or be based on the processing of special categories of data or criminal history records (previously sensitive personal data) unless:

39.8.1 we have the explicit consent of the individual; or

39.8.2 the processing is necessary for reasons of substantial public interest on the basis of EU / Member State law. This must be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and the interests of the individual; and

39.8.3 (in each case) suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

40. Enforcement.

40.1 If an individual disagrees that we have properly complied with a Right or we fail to respond they may apply to a Court for an order or complain to the ICO in each case requiring us to properly perform the Right.

40.2 If the Court or the ICO agrees with the individual it can:

40.2.1 40.2.1order us to properly carry out the Right and what steps are needed to do this; and

40.2.2 order us to notify third parties who we have passed the data onto of the Right;

40.3 A court can also award compensation to the individual for any damage they have suffered as a result of our non-compliance. The ICO can also impose a civil fine upon us. These fines can be very substantial.

41. Deleting Personal Data in the normal course.

41.1 We are only required to supply information in response to an exercise of Rights that was processed at the date of that request. However, we are allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of request in relation to a Right.

41.2 What we cannot do is amend or delete data because we do not want to supply it or because of the exercise of a Right.