Sports Centre

(Canons Enterprises Limited)

DATA PROTECTION POLICY

Policy Lead	MAC (MN)
Reviewed By	Directors
Date of Approval	14 May 2018
Authorised By	Directors
Date of Authorisation	14 May 2018
Date of Next Review	May 2019

CONTENTS

DATA PROTECTION POLICY

This policy complies with the General Data Protection Regulation 2018, Data Protection Bill 2017, the Privacy and Electronic Communications Regulations (2003), the Protection of Freedom Act 2012, and the relevant guidance and practice notes provided by the Information Commissioner's Office namely:

- Information Commissioner's CCTV Code of Practice
- Guidance on Children and the GDPR
- Guidance on Legitimate Interests
- Guidance on Consent
- Guidance on Direct Marketing

This policy can be made available in large print or other accessible format if required.

This policy should be read in conjunction with the following:

- Key Privacy Information
- Privacy Notice for Adult and Child users of the Canons Sports Centre
- Regulations for the user of the Canons Sports Centre

This policy is intended to provide information about how Canons Enterprises Limited, operating as the Canons Sports Centre ("Canons"), will use or "process" personal data about individuals including current and past members (and in some cases the parents of members), as well as Sports Centre users – all referred to in this policy as "Users" ("Child User" or "Adult User" will be used if appropriate). It applies in addition to Canons' regulations and any other information Canons may provide about a particular use of personal data.

Anyone who works for or acts on behalf of Canons (including staff, volunteers, directors and service providers) should also be aware of and comply with this policy and related documents.

The General Data Protection Regulation (GDPR) is an EU regulation which will take effect on 25th May 2018. The government has confirmed the UK's decision to leave the EU will not affect the commencement of the GDPR.

It should be noted that data protection should always take second place to safeguarding and child protection. If there is a potential conflict between the two competing requirements, the welfare of the child is paramount. For further information, see HM Government's non-statutory guidance 'Information sharing: Advice for practitioners providing safeguarding services to children, young people and carers' (March 2015).

1. DEFINITIONS
For the purposes of the GDPR:

Biometric Data – any personal data relating to the physical, physiological or behavioural characteristics of an individual which allows their unique identification.

Consent – freely given, specific, informed and explicit consent by statement or action signifying agreement to the processing of their personal data.

Data Concerning Health – any personal data related to the physical or mental health of an individual or the provision of health services to them.

Data Controller – the entity that determines the purposes, conditions and means of processing of personal data.

Data Erasure – also known as the Right to be Forgotten, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data and potentially have third parties cease processing of the data.

Data Portability – the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller.

Data Protection Impact Assessments (DPIAs) – tool to help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

Data Processor – the entity that processes data on behalf of the Data Controller.

Data Subject – a natural person whose personal data is processed by a controller or processor.

Encrypted Data – personal data that is protected through technological measures to ensure that the data is only accessible by those with specified access.

Personal Data – any information related to a natural person or data subject, that can be used directly or indirectly to identify the person.

Personal Data Breach – a breach of security leading to the accidental or unlawful access to, destruction, misuse etc. of personal data.

Privacy by Design – a principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.

Processing – any operation performed on personal data, whether or not by automated means, including collection, use, recording etc.

Pseudonymisation – substitutes the identity of the data subject in such a way that additional information is required to re-identify the data subject.

Right to be forgotten – also known as Data Erasure, it entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties cease processing of the data.

Right to Access/Subject Access Request – entitles the data subject to have access to, and information about, the personal data that a controller has concerning them.

Special Categories of Personal Data - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Supervisory Authority – The Information Commissioner's Office (ICO) is the Supervisory Authority for the United Kingdom.

2. RESPONSIBILITY FOR DATA PROTECTION

Whilst Canons is the Data Controller, the North London Collegiate School (NLCS) Director of IT will act as the Data Protection Lead on behalf of Canons and will endeavour to ensure that all personal data is processed in compliance with the GDPR. In the absence of the NLCS Director of IT, the NLCS Compliance Officer will act up as the Lead.

3. THE PRINCIPLES

There are six Principles of data protection in the GDPR. These Principles give people specific rights in relation to their personal data and place certain obligations on those organisations that are responsible for processing it.

1) Lawfulness, fairness and transparency
2) Purpose limitation
3) Data minimisation
4) Accuracy
5) Storage limitation
6) Integrity and confidentiality

Canons shall, so far as is reasonably practicable, comply with the Principles contained in the GDPR to ensure all personal data is:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation);
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regards to the purposes for which they are processed, are erased or rectified without delay (accuracy);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation);
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).

4. TYPES OF PERSONAL DATA PROCESSED BY CANONS

Canons may process a wide range of personal data about individuals including current and past Users as part of its operation, including by way of example:

- names, addresses, telephone numbers, e-mail addresses and other contact details;
- bank details and other financial information, e.g. about Users and parents of child Users who pay fees to Canons;
- dates of birth to identify the age of Users who would be entitled to student and young person discounts on membership;
- where appropriate, information about individuals' health or any special needs as they relate to activities undertaken in the Sports Centre;
- contact details for their next of kin for child Users;
- images of Users engaging in activities, taken and stored for the purposes of marketing Canons, and images captured by Canons' CCTV system.
- Generally, Canons receives personal data from the individual directly (or, in the case of child Users, from parents).

Canons may, from time to time, need to process "special categories of personal data" regarding individuals. This type of personal data is entitled to special protection under the GDPR, and will only be processed by Canons with the explicit consent of the appropriate individual for one or more specified purposes, except where relevant legal restrictions prohibit processing.

5. USE OF PERSONAL DATA BY CANONS

Canons will use (and where appropriate share with third parties, e.g. accident records and membership fees with NLCS) personal data about individuals for a number of purposes as part of its operations, including as follows:

- For the purposes of User applications to confirm the identity of prospective Users;

- To provide sporting, coaching and fitness services; monitoring Users' progress and fitness needs; and maintaining relationships with the Users and the Canons' community;
- For the purposes of management planning and forecasting, research and statistical analysis, and to enable NLCS and the relevant authorities to monitor Canons' performance;
- To receive information and references relating to applicants for employment and to provide references to potential employers of staff;
- To safeguard child welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so, for example for medical advice, insurance purposes or to the organisers of Canons activities;
- To monitor (as appropriate) use of Canons' IT and communications systems in accordance with NLCs's Safer Use of Technology Policy;
- To make use of photographic images of Users in Canons and NLCS publications, on Canons website and where appropriate on Canons' social media channels in accordance with Canons' policy on taking, storing and using images of children;
- For security purposes, and for regulatory and legal purposes (for example, child protection and health and safety) and to comply with its legal obligations; and
- Where otherwise reasonably necessary for Canons' purposes, including to obtain appropriate professional advice and insurance for Canons.

6. INDIVIDUAL RIGHTS

The GDPR provides the following rights for individuals (including children):

The right to be informed: Canons provides privacy notices which ensure transparency of processing, by setting out how Canons uses personal data.

The right of access: individuals have the right to access their personal data and supplementary information by making a 'Subject Access Request' (see Section 7). The right of access allows individuals to be aware of and verify the lawfulness of the processing.

The right to rectification: individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

The right to erasure/the right to be forgotten: this right enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to restrict processing: individuals have a right to 'block' or suppress processing of personal data under certain circumstances. For example, where an individual contests the accuracy of the personal data, where an individual has objected to the processing, when processing is unlawful and the individual opposes erasure and requests restriction instead etc.

The right to data portability: allows individuals to obtain and reuse their personal data for their own purposes across different services.

The right to object: individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Rights in relation to automated decision making and profiling: the GDPR has provisions on:

- automated individual decision-making ie, making a decision solely by automated means without any human involvement; and
- profiling ie, automated processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process.

For detailed information on the above rights please go to: https://ico.org.uk/for organisations/ guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Individuals wishing to exercise any of the above rights should write to the Data Protection Lead at Canons address, or via email, at dataprotection@nlcs.org.uk setting out which right/s they wish to exercise and the reasons for doing so. Canons will provide a written response and/or where applicable will action the request within one month of receipt of the written applications.

7. RIGHTS OF ACCESS TO PERSONAL DATA ("SUBJECT ACCESS REQUEST")

Under the GDPR, individuals have the right to obtain:

- confirmation from Canons that their data is being processed;
- access to their personal data; and
- certain other supplementary information, for example, the purposes of the processing, the categories of personal data concerned, to whom the personal data has been or will be disclosed etc.

Any individual wishing to access their personal data should put their request in writing to the Data Protection Lead at Canons address or email the Data Protection Lead at: dataprotection@nlcs.org.uk.

Canons will verify the identity of the individual making the subject access request by requesting a valid form of photographic id e.g., copy of passport or driving licence.

Canons will endeavour to respond to any such written requests, known as "subject access requests", as soon as is reasonably practicable and at the latest within one month of receipt of the request. If the subject access request is complex Canons can extend the period of compliance by a further two months. The individual making the request will be informed of

the extension within one month of the receipt of the subject access request, and will be provided with an explanation as to why the extension is necessary.

Canons will provide this information free of charge however, a reasonable fee may be charged where the request is manifestly unfounded or excessive, particularly if it is repetitive, and where requests are made for further copies of the same information.

Where Canons processes a large quantity of information about an individual, the GDPR permits Canons to ask the individual making a SAR to specify the information their request relates to. Canons will be greatly assisted in dealing with SAR's if individuals are able to provide a rationale for making the request.

Canons is entitled to refuse to respond to subject access requests where requests are manifestly unfounded or excessive, particularly if it is repetitive. The individual making the request will, without undue delay and at the latest within one month of the receipt of the subject access request, be provided with an explanation regarding the reason/s for refusal. The individual will also be informed of their right to complain to the supervisory authority and to a judicial remedy.

The process for handling Subject Access Requests is at **Appendix 1**.

8. WHOSE RIGHTS

The rights belong to the individual to whom the data relates. However, Canons will in some cases rely on parental consent to process personal data relating to a Child User (if consent is required) unless, given the nature of the processing in question, and the child's age and understanding, it is more appropriate to rely on the Child User's consent. Parents should be aware that in such situations they may not be consulted.

In general, Canons will assume that Child Users consent to disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the child's activities, progress and behaviour, and in the interests of the child's welfare, unless, in Canons' opinion, there is a good reason to do otherwise.

However, where a Child User seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, Canons will maintain confidentiality unless, in Canons' opinion, there is a good reason to do otherwise; for example where Canons believes disclosure will be in the best interests of the Child User or other Users.

9. DATA ACCURACY AND SECURITY

Canons will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must notify Canons in writing of any changes to information held about them.

An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations) and may do so by contacting the

Data Protection Lead, in writing, at *Canons Sports Centre, North London Collegiate School, Canons Drive, Edgware, HA8 7RJ*, or via email, at dataprotection@nlcs.org.uk.

Canons will take appropriate technical and organisational steps to ensure the security of personal data about individuals. All staff will be made aware of this policy and their duties under the GDPR.

10. REPORTING DATA BREACHES

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In brief, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

In the event of a breach or (suspected breach) the member of staff must inform the Data Protection Lead, without delay, providing as much information as possible. The Data Protection Lead will establish whether a personal data breach has occurred and, if so, promptly take the necessary steps to address it. The Data Protection Lead will notify the NLCS Operations and Estates Bursar (a Canons Director) in the first instance.

If a personal data breach has occurred the Data Protection Lead and the NLCS Operations and Estates Bursar will establish the likelihood and severity of the resulting risk to the individual/s rights and freedoms. If it is deemed that there will be a risk, the Data Protection Lead or the NLCS Operations and Estates Bursar will notify the Information Commissioner's Office (ICO), without undue delay, and not later than 72 hours after having become aware of the breach. If it is unlikely that there will be a risk to individual/s rights and freedoms the breach will not be reported to the ICO.

If there is a likelihood of a *high* risk to the individual/s rights and freedoms the Data Protection Lead or the NLCS Operations and Estates Bursar will also report the breach, without undue delay, to the individual/s who have been affected. Examples of high risk situations include, amongst other things, individual/s suffering discrimination, damage to reputation, financial loss, other significant economic or social disadvantage as a consequence of the breach.

The Data Protection Lead will also notify the Designated Safeguarding Leads if the breach or suspected breach relates to Child User data.

The process for handling a Personal Data Breach is at **Appendix 2**.

11. DATA RETENTION AND STORAGE GUIDELINES

In these guidelines, "record" means any document or item of data which contains evidence or information relating to Canons, its staff or Users. Some of this material will contain personal data of individuals as defined in the GDPR. Many, if not most, new and recent

records will be created, received and stored electronically. Others such as certificates, registers or older records will be original paper documents. The format of the record is less important than its contents and the purpose for keeping it.

12. STORAGE OF RECORDS

Digital records:

Digital records can be lost or misappropriated in huge quantities very quickly. Access to special categories of personal data, or any large quantity of data, should as a minimum be password protected and held on a limited number of devices only, with passwords provided on a need to know basis and regularly changed.

Emails, whether retained electronically or printed out as part of a paper file, are also records and may be particularly important whether as disclosable documents in litigation, or as representing personal data of the sender (or subject) for data protection/data privacy purposes. Again, the format is secondary to the content and the purpose of keeping the document as a record.

Staff should bear in mind that documents and records, including emails, may be disclosable due to litigation, investigation or the receipt of a subject access request, and therefore should be accurate and professional.

Paper records:

Paper records are only classed as personal data if held in a "relevant filing system". This means organised, and/or indexed, such that specific categories of personal information relating to a certain individual are readily accessible and thus searchable as a digital database might be. By way of example, an alphabetical personnel file split into marked dividers will likely fall under this category but a merely chronological file of correspondence may well not. Where personal information is contained on print-outs taken from electronic files, the data has already been processed by Canons and falls within the GDPR.

Paper records should be stored in a secure, dry, cool and reasonably ventilated area.

Archiving and the destruction of records:

Staff given specific responsibility for the management of records must ensure, as a minimum, the following:

- That records, whether electronic or hard copy, are stored securely, including if possible, with encryption, so that access is available only to authorised persons and the records themselves are available when required and (where necessary) searchable;

- That important records, and large or sensitive personal databases, are not taken home or, in respect of digital data, carried or kept on portable devices unless absolutely necessary;

- Back-ups or migration should be approached in line with general NLCS policy such as professional storage solutions or IT systems and not individual ad hoc action;

- That reviews are conducted on a regular basis, in line with the guidance below, to ensure all information being kept is still relevant and, in the case of personal data, necessary for the purposes for which it is held (and if so, that it is accurate and up to date) and;

- That all destruction or permanent erasure of records, if undertaken by a third party, is carried out securely with no risk of the re-use or disclosure, or reconstruction, of any records or information contained in them.

A table summarising information retention periods is at **Appendix 3.**

13. CCTV

The Closed Circuit Television System (the CCTV System) is administered and managed by NLCS, which acts as the Data Controller.

All fixed cameras are in plain sight on Canons premises and Canons does not routinely use CCTV for covert monitoring or monitoring of private property outside Canons grounds.

Canons' purposes of using the CCTV System are set out below and, having fully considered the privacy rights of individuals, Canons believes these purposes are all in its legitimate interests. Data captured for the purposes below will not be used for any commercial purpose.

Objectives of the System

- To protect Users, staff, volunteers, visitors and members of the public with regard to their personal safety.

- To protect Canons buildings and equipment, and the personal property of Users, staff, volunteers, visitors and members of the public.

- To support the police and community in preventing and detecting crime, and assist in the identification and apprehension of offenders.

- To monitor the security and integrity of Canons site and deliveries and arrivals.

- To monitor staff and contractors when carrying out work duties.

- To monitor and uphold discipline among Users in line with Canons Rules, which are available on request.

Positioning

Locations have been selected, both inside and out, that Canons reasonably believes require monitoring to address the stated objectives.

Adequate signage has been placed in prominent positions to inform staff and Users that they are entering a monitored area.

No images will be captured from areas in which individuals would have a heightened expectation of privacy, including changing and washroom facilities.

No images of public spaces will be captured except to a limited extent at site entrances.

Maintenance

The CCTV System will be operational 24 hours a day, every day of the year. The NLCS Estates Manager will check and confirm that the CCTV System is properly recording and that cameras are functioning correctly, on a regular basis.

The CCTV System is checked weekly by NLCS Schoolkeepers and serviced no less than annually.

Supervision of the System

The overall responsibility for the CCTV system lies with the NLCS Operations and Estates Bursar.

Staff authorised by the NLCS Operations and Estates Bursar to conduct routine supervision of the CCTV System may include NLCS Estates Manager, NLCS Schoolkeepers, supervisors at Canons Sports Centre and relevant staff on duty.

Images will be viewed and/or monitored in a suitably secure and private area to minimise the likelihood of or opportunity for access to unauthorised persons.

Storage of Data

The day-to-day management of images will be the responsibility of the NLCS Estates Manager or such suitable person as the NLCS Estates Manager shall appoint in his absence.

Images will be stored for a maximum of 30 days and automatically over-written unless Canons considers it reasonably necessary for the pursuit of the objectives outlined above, or if lawfully required by an appropriate third party such as the police or local authority.

Where such data is retained, it will be retained in accordance with the GDPR and this policy. Information including the date, time and length of the recording, as well as the locations covered and groups or individuals recorded, will be recorded in the system log book.

Access to Images

Access to stored CCTV images will only be given to authorised persons, under the direction of the Operations and Estates Bursar, in pursuance of the above objectives (or if there is some other overriding and lawful reason to grant such access).

Individuals also have the right to access personal data Canons holds on them, including information held on the CCTV System, if it has been kept. Canons will require specific details including at least to time, date and camera location before it can properly respond to any such requests. This right is subject to certain exemptions from access, including in some circumstances where others are identifiable.

The Operations and Estates Bursar must satisfy himself of the identity of any person wishing to view stored images or access the system and the legitimacy of the request. The following are examples when the Operations and Estates Bursar may authorise access to CCTV images:

- Where required to do so by NLCS's Headmistress/Chief Operating Officer, the Police or a relevant statutory authority;
- To make a report regarding suspected criminal behaviour;
- To enable the Designated Safeguarding Lead or her appointed deputy to examine behaviour which may give rise to any reasonable safeguarding concern;
- To assist Canons in establishing facts in cases of unacceptable User behaviour;
- To data subjects (or their legal representatives) pursuant to a subject access request;
- To Canons' insurance company where required in order to pursue a claim for damage done to insured property; or
- In any other circumstances required under law or regulation.

Where images are disclosed a record will be made in the system log book including the person viewing the images, the time of access, the reason for viewing the images, the details of images viewed and a crime incident number (if applicable).

Where images are provided to third parties, wherever practicable, steps will be taken to obscure images of non-relevant individuals.

The CCTV Footage Access Request form is at **Appendix 4**.

Other CCTV systems

Canons does not own or manage third party CCTV systems, but may be provided by third parties with images of incidents where this in line with the objectives of Canons' own CCTV policy and/or its Regulations.

14. QUERIES AND COMPLAINTS

Any comments or queries on this policy, or in relation to NLCS/CANONS' CCTV System, should be referred to the Data Protection Lead at *Canons Sports Centre, North London Collegiate School, Canons Drive, Edgware, HA8 7RJ*, or via email, at: dataprotection@nlcs.org.uk .

If an individual believes that Canons has not complied with this policy or acted otherwise than in accordance with the GDPR, they should utilise Canons' Concerns & Complaints procedure and should also notify the Data Protection Lead. The individual can also contact the Information Commissioner's Office details of which can be found here: https://ico.org.uk/concerns/

15. MONITORING AND REVIEW

The Directors of Canons and the Data Protection Lead will monitor and evaluate the effectiveness of this policy, and associated procedures. The policy will be reviewed every two years or more frequently if changes to legislation, regulation or statutory guidance so require.

Appendix 1:

SUBJECT ACCESS REQUESTS

PERSONAL DATA:

Personal data constitutes any information related to a natural person or 'Data Subject' that can be used to directly or indirectly identify the person. This can be anything from a name, photo, email address, bank details, posts on social networking websites, medical information, computer IP address etc.

RIGHT OF ACCESS:

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

Under the General Data Protection Regulation (GDPR), individuals have the right to obtain:

- confirmation that their personal data is being processed;
- access to their personal data; and
- other supplementary information - for example, the purposes of the processing, the categories of personal data concerned, to whom the personal data has been or will be disclosed etc.

WHAT TO DO IF YOU RECEIVE A SUBJECT ACCESS REQUEST (SAR):

- If you receive a verbal request from an individual to access their personal data please ask the individual to put their SAR in writing and email the same to the Data Protection Lead at dataprotection@nlcs.org.uk. Alternatively the SAR can be posted to the Data Protection Lead at *Canons Sports Centre, North London Collegiate School, Canons Drive, Edgware, HA8 7RJ*, ensuring the envelope and correspondence is clearly marked for the attention of the Data Protection Lead.

- If you receive a written SAR, or what you believe may be a SAR, immediately notify and forward the request to the Data Protection Lead as Canons is required to respond within a strict timescale.

THE DATA PROTECTION LEAD:

- The Data Protection Lead will establish whether the request is a SAR.
- If the request is considered to be a SAR the identity of the person making the SAR must be verified using 'reasonable means'.
- The Data Protection Lead will liaise with the relevant member/s of staff to collate the necessary information.
- The information must be provided without delay and at the latest within one month of receipt. This can be extended by a further two months where requests are complex or numerous. If this is the case the individual making the SAR must be informed within one month of the receipt of the request and an explanation provided as to why the extension is necessary.

- The Data Protection Lead will consider whether information can be withheld/redacted. For example, information about another person may not always be made available to the individual making the SAR.
- The information will be provided free of charge. A 'reasonable fee' can be charged where a request is manifestly unfounded or excessive, particularly if it is repetitive, or for further copies of the same information.
- Where requests are manifestly unfounded or excessive Canons can refuse to respond. If this is the case the individual making the SAR must be provided with an explanation and informed of their right to complain to the Information Commissioner's Office.

Appendix 2:

PROCEDURE IN THE EVENT OF A PERSONAL DATA BREACH

(to be read in conjunction with Canons' Data Protection policy)

1. Upon the first employee becoming aware of the breach

    - *Am I the relevant person at the organisation? If not, immediately notify your line manager and the Data Protection Lead.*

2. Initial assessment (by Canons Sport Centre Manager, NLCS IT support team and NLCS Data Protection Lead), containment and recovery – first few hours:

    - *How long has the breach been active, what data was involved and how far has it got?*
    - *What immediate steps can be taken to prevent it going further? Consider:*
        - *if a cyber breach, involve NCLS's IT personnel from the outset;*
        - *if staff members are involved, can they be contacted to give reassurances;*
        - *if e.g. Royal Mail, courier, IT or other contractors are involved, can they assist;*
        - *are specialists needed: forensic IT consultants, crisis management PR, legal etc.*

The following and all subsequent actions will be undertaken by the NLCS Data Protection Lead (Director of IT) / the Operations and Estates Bursar (as Director of Canons Enterprises Ltd) and/or the NLCS Chief Operating Officer:

3. Initial notification where required, ongoing assessment of risk and mitigation – first 72 hours

    - *Build up a more detailed picture of the risk and reach of the security breach:*
        - *how many have been affected?*
        - *was any special category/sensitive personal data involved – e.g., health, criminal convictions?*
        - *was financial data involved and/or is there a risk of identify fraud?*
    - *Identify if a crime has been committed and involve police or cyber fraud unit.*
    - *Assess if insurers need notifying (major loss, crime, or possible legal claim(s))*
    - *Decide if the likely risk of harm to the data subjects:*
        - *is sufficient to require a full <u>or</u> preliminary notification to the ICO; and*
        - *is sufficiently serious to require communication to affected individuals*
    - *If not, is this a matter we can document but deal with internally?; or*
    - *If so, what can we usefully tell the ICO and/or individuals at this stage?*
        - *e.g. provide fraud or password advice, offer counselling etc.*

4. Ongoing evaluation, monitoring and remediation:

    - *Continue to monitor and assess possible consequences (even if apparently contained).*
    - *Keep the ICO and/or those affected informed as new information becomes available.*

- *Tell the ICO and/or those affected what you are doing to remediate and improve practice.*
- *Begin process of review internally:*
    - *how did this happen? What could we have done better?*
    - *would training or even disciplinary action be justified for staff members?*
    - *were our policies adequate, and/or adequately followed?*
    - *if our contractors were involved (e.g. systems providers), did they respond adequately? Do we have any remedies against them if not?*

5. Record keeping and putting outcomes into practice:

    - *Keep a full internal record, whether or not the matter was reported or resulted in harm.*
    - *Log this record against wider trends and compare with past incidents.*
    - *Make sure all past outcomes were in fact put into practice.*
    - *Ensure any recommendations made by, or promised to, the ICO are actioned.*
    - *If reported to the ICO, notify the Charity Commission.*
    - *Review policies and ensure regular (or specific, if required) training is actually completed.*

Noting the responsibilities outlined above: Serious breaches should be reported to the ICO using the security breach helpline on 0303 123 1113 (open Monday to Friday, 9am to 5pm). Select option 3 to speak to staff who will record the breach and give advice.

Or, use the security breach notification form, which should be sent to the email address: casework@ico.org.uk or by post to the ICO office address: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

The security breach notification form can be found here:

https://ico.org.uk/media/fororganisations/documents/2666/security_breach_notification_form.doc

Appendix 3:

TABLE OF RETENTION PERIODS

Type of Record/Document	Retention Period
INDIVIDUAL USERS RECORDS	***NB – this will generally be personal data***
• Application / Information forms	1 year following last registered attendance at Canons
• Special needs or medical conditions (*to be risk assessed individually*)	As above
• Direct Debit Mandates	As above
SAFEGUARDING	
• Policies and procedures	Keep a permanent record of historic policies
• Accident / Incident reporting	Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available.
• Child Protection files	If a referral has been made / social care have been involved or child has been subject of a multi-agency plan – indefinitely. If low level concerns, with no multi-agency act – apply applicable NLCS low-level concerns policy rationale (this may be 25 years from date of birth OR indefinitely).
CORPORATE RECORDS	
• Certificates of Incorporation	Permanent (or until dissolution of the company)
• Shareholder resolutions	Minimum – 10 years
• Register of Members/Shareholders	Permanent (minimum 10 years for ex-members/shareholders)
• Annual reports	Minimum – 6 years
DIRECTORS' RECORDS	
• Minutes, Notes and Resolutions of Boards Meetings	Permanent
• Register of Directors	Permanent

Type of Record/Document	Retention Period
• Declaration of Interest forms	Permanent
ACCOUNTING RECORDS [3]	
• Accounting records	Minimum – 3 years for private UK companies (except where still necessary for tax returns)
• Tax returns	Minimum – 6 years
• VAT returns	Minimum – 6 years
• Budget and internal financial reports	Minimum – 3 years
CONTRACTS AND AGREEMENTS	
• Signed or final/concluded agreements (*plus any signed or final/concluded variations or amendments*)	Kept indefinitely
• Deeds (or contracts under seal)	Kept indefinitely
INTELLECTUAL PROPERTY RECORDS	
• Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, e.g., trade marks); otherwise expiry of right plus minimum of 7 years.
• Assignments of intellectual property to or from Canons	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).
• IP / IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement
EMPLOYEE / PERSONNEL RECORDS	***NB this will almost certainly be personal data***
• Single Central Record of employees	Keep a permanent record of all mandatory checks that have been undertaken (not certificate)
• Contracts of employment	7 years from effective date of end of contract

Type of Record/Document	Retention Period
• Employee appraisals or reviews	Duration of employment plus minimum of 7 years
• Staff personnel file	As above, but do not delete any information which may be relevant to historic safeguarding claims.
• Payroll, salary, maternity pay records	Minimum – 6 years
• Pension or other benefit schedule records	Possibly permanent, depending on nature of scheme
• Job application and interview/rejection records (unsuccessful applicants)	Minimum 3 months but no more than 1 year
• Immigration records	Minimum – 4 years
• Health records relating to employees	7 years from end of contract of employment
INSURANCE RECORDS	
• Insurance policies (will vary – private, public, professional indemnity)	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim.
• Correspondence related to claims/ renewals/ notification re: insurance	Minimum – 7 years
ENVIRONMENTAL & HEALTH RECORDS	
• Maintenance logs	10 years from date of last entry
• Accidents to children	25 years from birth (unless safeguarding incident)
• Accident at work records (staff)	Minimum – 4 years from date of accident, but review case-by-case where possible
• Staff use of hazardous substances	Minimum – 7 years from end of date of use
• Risk assessments (carried out in respect of above)	7 years from completion of relevant project, incident, event or activity.

Appendix 4:

CCTV FOOTAGE ACCESS REQUEST

The following information is required before Canons/NLCS can provide copies of or access to CCTV footage from which a person believes they may be identified.

Please note that CCTV footage may contain the information of others that needs to be protected, and that Canons typically deletes CCTV recordings after a 30 day period.

Name and address: (proof of ID may be required)	
Description of footage (including a description of yourself, clothing, activity etc.)	
Location of camera	
Date of footage sought	
Approximate time (give a range if necessary)	

Signature*……

Print Name…….. Date ……..

*** NB if requesting CCTV footage of a child under 13, a person with parental responsibility should sign this form. For children 13 or over, the child's authority or consent must be obtained except in circumstances where that would clearly be inappropriate and the lawful reasons to provide to the parent(s) outweigh the privacy considerations of the child.**