Data Protection Policy

Version date: March 2020

Next review due: June 2021

Data Protection Policy

Contents

Lacrosse Scotland, Caledonia House, South Gyle, Edinburgh, EH12 9DQ
w. www.lacrossescotland.com e. admin@lacrossescotland.com
Registered Company SC282483

Data Protection Policy

Foreword and Definitions

Lacrosse Scotland is committed to complying with data protection law and to respecting the privacy rights of individuals. This Data Protection Policy, henceforth as **Policy** applies to all of our staff, workers, officials, directors, volunteers and consultants, henceforth as **Workers**.

This 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 clubs and organisations associated with Lacrosse Scotland.

References in this Policy to "us", "we", "ourselves" and "our" are to Lacrosse Scotland, whilst references to "you", "yourself" and "your" are to every person whom this Policy applies.

We recognise that you have an important role to play in achieving these aims. It is therefore your responsibility 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 it 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/ Finance Director or any other Lacrosse Scotland Official.

Who is responsible for data protection?

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.

Why do we have a data protection policy?

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.

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

Status of this Policy and the implications of breach.

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.

If you do not comply with data protection laws and/or this Policy, then you are encouraged to report this fact immediately to our DPO/ Chairperson. 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.

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/ Chairperson. 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.

Other consequences

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

For you:

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.
2. **Criminal sanctions:** Serious breaches could potentially result in criminal liability.
3. **Investigations and interviews:** Your actions could be investigated and you could be interviewed in relation to any non-compliance.

For the Organisation:

1. **Criminal sanctions:** Non-compliance could involve a criminal offence.
2. **Civil Fines:** These can be up to Euro 20 million or 4% of group worldwide turnover whichever is higher. These amounts are very substantial.
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. **Court orders:** These may require us to implement measures or take steps in relation to, or cease or refrain from, processing personal data.
5. **Claims for compensation:** Individuals may make claims for damage they have suffered as a result of our non- compliance.
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.
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.

Data protection laws

The Data Protection Act 2018 ("**DPA 2018**") is the UK's implementation of the General Data Protection Regulation ("**GDPR**") and applies to any personal data that we process.

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).

Keywords in relation to data protection

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

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).

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).
3. **Data subject** is the living individual to whom the relevant personal data relates.
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.
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. Lacrosse Scotland does fulfill the basic criteria (as defined by the Information Commissioner's Office, henceforth as ICO) to qualify as Data Collector.
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.

Commented [1]: This is on an assumption that LS does collect members' data, i.e. decides how and why to collect and use the data. https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/

Outline

The data protection laws require us to:

1. only process personal data for certain purposes;
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).
3. provide certain information to those individuals about whom we process personal data. You will have received one of these from us through our Privacy Policy;
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
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.

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

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.

Data protection principles and what you must do

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

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

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

2. 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.
3. 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 DPO/ Chairperson.

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

1. You must only process personal data for purposes for which it was collected e.g. if you have taken a member's details to forward information to them around our events, you must not use it for sending marketing information of our branded t-shirts.
2. If personal data is to be processed for another purpose, the individual must be informed of that purpose and consent to it.
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.

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

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.
2. If we do not collect sufficient personal data to utilise it for its intended purpose, it should be securely deleted or destroyed.
3. If more personal data than is required has been collected, the unnecessary personal data should be securely deleted or destroyed.
4. When collecting personal data or recording personal data, think whether it is in fact needed for the purpose for which it is collected.

accurate and where necessary kept up to date;

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

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

1. You must delete data no longer required to fulfil the purposes for which it was originally collected.
2. Retention periods for data will be set out in our standard privacy notice provided to the individual.
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.

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

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

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.
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.

Data subject rights

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

1. The rights to access their personal data, usually referred to as a **subject access request**;
2. The right to have their personal data rectified;
3. The right to have their personal data erased, usually referred to as **the right to be forgotten**;
4. The right to restrict processing of their personal data;
5. The right to object to receiving direct marketing materials;
6. The right to portability of their personal data;
7. The right to object to processing of their personal data; and
8. The right to not be subject to a decision made solely by automated data processing.

Not all of these rights are absolute rights, some are qualified and some only apply in specific circumstances.

In case of a request to exercise data subject right - please refer to **LS Data Subject Right Request** document.

Your main obligations

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

1. Treat all personal data with respect;
2. Treat all personal data how you would want your own personal data to be treated;
3. Immediately notify your line manager or our DPO/ Chairperson if 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;
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
5. Immediately notify our DPO/ Chairperson 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].

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.

Your activities

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.

Areas and activities particularly affected by data protection laws include Human Resources, payroll, member database management and support, sales, marketing and promotions, health and safety, finance, performance and participation.

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.

Personal data

Data will relate to an individual and therefore be their personal data if it:

1. identifies the individual. For instance, names, addresses, telephone numbers and email addresses;
2. its content is about the individual personally. For instance, medical records, credit history, a recording of their actions, or contact details;
3. relates to property of the individual, for example their home, their car or other possessions;
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);
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;
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;
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;
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
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).

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.

Examples of information likely to constitute personal data:

1. Unique names;
2. Names together with email addresses or other contact details;
3. Job title and employer (if there is only one person in the position);
4. Video - and photographic images;
5. Information about individuals obtained as a result of Safeguarding checks;
6. Medical and disability information;

7. Member profile information (e.g. marketing preferences); and
8. Financial information and accounts (e.g. information about expenses and benefits entitlements, income and expenditure).

Examples of information unlikely to constitute personal data:

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
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).

Lawful basis for processing

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

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

1. the data subject has given their consent to the processing;
2. the processing is necessary for the performance of a contract with the data subject (e.g. executing their Lacrosse Scotland membership);
3. the processing is necessary for compliance with a legal obligation to which the data controller is subject; or
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.

Special category data

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.

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.

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

1. the individual has given their explicit consent to the processing;
2. the processing is necessary for the performance of our obligations under employment law;
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;
4. the processing relates to information manifestly made public by the data subject;
5. the processing is necessary for the purpose of establishing, exercising or defending legal claims; or
6. the processing is necessary for the purpose of preventive or occupational medicine or for the assessment of the working capacity of the employee.

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

1. ensure that either the individual has given their explicit consent to the processing; or
2. ensure that our processing of those criminal records history is necessary under a legal requirement imposed upon us.

We would normally only expect to process special category personal data or criminal records history data usually in a Human Resources context and also in the context of our members/athletes/coaches/volunteers etc. for e.g. monitoring performance, drug and alcohol testing, health and safety requirements, safeguarding checks, classification, facilitation and accreditation etc.

When do we process personal data?

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.

Examples of processing personal data might include:

1. Using personal data to correspond with members and participants;
2. Holding personal data in our databases or documents; and
3. Recording personal data in personnel or member files.

What does this mean?

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.

Practical matters

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:

1. Do not take personal data out of the organisation's premises (unless absolutely necessary).
2. Do not disclose your unique logins and passwords for any of our IT systems to anyone.
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 phones, laptops, tablets, memory sticks etc.
4. Never leave any items containing personal data in unsecure locations, e.g. in a car on your drive overnight and this would include paper files, mobile phones, laptops, tablets, memory sticks etc.
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.
6. Do encrypt laptops, mobile devices and removable storage devices containing personal data.
7. Do lock laptops, files, mobile devices and removable storage devices containing personal data away and out of sight when not in use.
8. Do password protect documents and databases containing personal data.
9. Never use removable storage media to store personal data unless the personal data on the media is encrypted.
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.

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. Do dispose of any materials containing personal data securely, whether the materials are paper based or electronic.
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.
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.
15. Do challenge unexpected visitors or employees accessing personal data.
16. Do not leave personal data lying around, store it securely.
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 only first names to preserve confidentiality.
18. If taking down details or instructions from a member 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.
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.
20. Do not transfer personal data to any third party without prior written consent of your line manager or our DPO/ Chairperson.
21. Do notify your line manager or our DPO/ Chairperson immediately of any suspected security breaches or loss of personal data.
22. If any personal data is lost, or any devices or materials containing any personal data are lost, report it immediately to our DPO/ Chairperson. [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.

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 DPO/ Chairperson.

Queries

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