Data Protection and GDPR Policy

Document date	2023-01-04	Document version No.	Final	Next Review Date	
Prepared by	S Morris	Position	Chairman	Date of Approval	2023.1.23

Contents

Part I – Overview of what the Data Protection Act 2018 means for Kingsclere Village Club

Data Protection Act 2018 has revolutionised data protection. It applies to all organisations in the same way, regardless of size, and is onerous.

In essence, personal data is to be looked after as if is it a valuable asset. The Act requires

1. Personal data to be processed only in permitted purposes
2. Data to be processed in accordance with statutory principles
3. Organisations give effect to the rights granted to individuals
4. Data transferred to third countries
5. Data breaches are be notified – and penalties potentially apply
6. Organisations to train its staff, plus risk assess the personal data it processes to ensure its use of data and retention is permitted by the Act and that it is secure.

1. **Permitted Purposes**

(a) Consent for a specific purpose

(b) Necessary for the performance of a contract

(c) Compliance with a legal obligation

(d) Necessary to protect the vital interests of the data subject or another living person

(e) Necessary for the performance of a task carried out in the public interest or in the exercise of official authority

(f) Necessary for the legitimate interests pursued by the controller or a third party, unless overridden by the interests of fundamental rights of the data subject which require protection of personal data.

2. Statutory Processing Principles

(a) lawfulness, fairness and transparency' - ie, processed lawfully, fairly and in a transparent manner

(b) purpose limitation - ie, collected for specified, explicit and legitimate purposes

(c) data minimisation – ie, adequate, relevant and limited to what is necessary in relation to the purposes for processing

(d) accuracy – ie, kept up to date and inaccuracies are erased or rectified without delay

(e) storage limitation - 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. Longer retention is permitted for archiving in the public interest, scientific or historical research purposes or statistical purposes in accordance with UK GDPR subject to implementation of the appropriate technical and organisational statutory measures to safeguard the rights and freedoms of the data subject

(f) integrity and confidentiality – ie, appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage,

(g) accountability – ie, a data controller will be in place and be able to demonstrate compliance.

3. Individual Rights

(a) Transparency and modalities – if asked to be told what personal information we have about them, give them a copy and state how we obtained it.

(b) Information and access to personal data – **at the point of collection,** be provided with specified and extensive information about how their data is processed lawfully, their rights and how to enforce them. See the Checklist for Compliance with Individuals' Rights to Information and Access to Personal Data provided below

(c) Rectification, erasure and restriction - requests to be actioned without unreasonable delay ie, within one month. Can be refused on certain grounds

(d) Right to object to certain purposes and automated individual decision-making - those purposes are processing based on legitimate interests or public interest; direct marketing; and processing for purposes of scientific/historical research and statistics.

4. International Transfers

The 2018 Act imposes restrictions on the transfer of data outside of the UK to ensure that individual rights are not eroded.

We are permitted to transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

Adequate safeguards may be provided for by:

(1) A transfer to a third country that is subject to an adequacy decision

(2) An international data transfer agreement

(3) A legally binding and enforceable instrument between public authorities or bodies;

(4) binding corporate rules (agreements governing transfers made between organisations within in a corporate group);

(5) standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;

(6) compliance with an approved code of conduct approved by a supervisory authority;

(7) certification under an approved certification mechanism as provided for in the GDPR;

(8) contractual clauses agreed authorised by the competent supervisory authority; or

(9) provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

We will only transfer personal data outside of the UK if one of these safeguards is in place or if the transfer

is

(1) made with the individual's informed consent;

(2) necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;

(3) necessary for the performance of a contract made in the interests of the individual between the controller and another person;

(4) necessary for important reasons of public interest;

(5) necessary for the establishment, exercise or defence of legal claims;

(6) necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or

(7) made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

5. Data Breaches

Personal data breaches can include:

(1) access by an unauthorised third party;

(2) deliberate or accidental action (or inaction) by a controller or processor;

(3) sending personal data to an incorrect recipient;

(4) computing devices containing personal data being lost or stolen;

(5) alteration of personal data without permission; and

(6) loss of availability of personal data.

We need to recognise breaches and act quickly to let data subjects know how to protect themselves, and decide whether the ICO needs to be notified. Notification must be within 72 hours. If we take longer than this, we must give reasons for the delay.

Data subjects may be entitled to compensation if they have experienced harm as a result of the breach. It will not be awarded simply for distress.

As an organisation we can be fined by the ICO for non-compliance. The fines are onerous – but are a means of last resort. We should never allow things to get to this point.

6. Organisational Response

As an organisation we need to demonstrate compliance, and in part this means having the following in place:

Data audit - assessment of use and security

- Providing Staff Training
- Data Controller
- Data Protection Officer

- Data Protection Registration
- Privacy Notices

Part II ICO Guidelines for Implementation

1 Checklist for Compliance with Individuals' Rights to Information and Access to Personal Data

When collecting personal data, we are under a duty to give:

1. the identity and the contact details of the controller and, where applicable, of the controller's representative;
2. the contact details of the data protection officer, where applicable;
3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4. if the purpose of processing is for the legitimate interests of the organisation (or a third party) what those legitimate interests are;
5. the recipients or categories of recipients of the personal data, if any;
6. whether personal data is going to be transferred to a third country or international organisation, and whether this is approved (or not) by the European Commission; plus, a reference to the safeguards or where they are available
7. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
8. that there are rights to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
9. where the processing is based on consent, or concerns special personal data (race, sex, sexual orientation, genetic material) the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
10. the right to lodge a complaint with a supervisory authority;
11. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
12. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
13. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

2. Dealing with a Request for Rectification, and Grounds for Refusal

On receiving a request for rectification, we will take reasonable steps to satisfy ourselves that the data is accurate and to rectify the data if necessary, taking into account the arguments and evidence provided by the data subject.

A formal response will be provided within one month.

We are entitled to refuse to comply with a request for rectification if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If we consider that a request is manifestly unfounded or excessive, we can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

And will justify that decision.

We will base the reasonable fee on the administrative costs of complying with the request. If we decide to charge a fee the individual will be contacted without undue delay and within one month. We are entitled not to comply with the request until the fee has been received.

The Data Protection Act 2018 provides additional exemptions:

1. Crime, law and public protection
2. Regulation, parliament and the judiciary
3. Journalism, research and archiving
4. Health, social work, education and child abuse
5. Finance, management and negotiations
6. References and exams
7. Subject access requests about other people
8. National security and defence

If we consider thar the request fall within one of these we will follow the ICO's guidance on a case-by-case basis.

3. Dealing with Requests for Erasure and Grounds for Refusal

Individuals have the right to have their personal data erased if:

(1) the personal data is no longer necessary for the purpose which we originally collected or processed it for;

(2) we are relying on consent as our lawful basis for holding the data, and the individual withdraws their consent;

(3) we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;

(4) we are processing the personal data for direct marketing purposes and the individual objects to that processing;

(5) we have processed the personal data unlawfully (ie, in breach of the lawfulness requirement of the 1st

principle);

(6) we have to do it to comply with a legal obligation; or

(7) we have processed the personal data to offer information society services to a child.

If the request related to information gained from a child weight shall be given to their request even if they are now an adult.

We will tell other organisations about the erasure of personal data in the following two situations:

- the personal data has been disclosed to others; or
- the personal data has been made public in an online environment (for example on social networks, forums or websites).

If we have disclosed the personal data to others, we will contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, we will also inform the individuals about these recipients.

Where personal data has been made public in an online environment reasonable steps will be taken to inform other controllers who are processing the personal data to erase links to, copies or replication of that data. When deciding what steps are reasonable, we will take into account available technology and the cost of implementation.

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

The 2018 Act also specifies two circumstances where the right to erasure will not apply to special category data: This is not relevant to us as we do not collect data of this nature.

4. Dealing with Requests for Restriction and Grounds for Refusal

This means that in certain circumstances an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

The circumstances are:

(1) the individual contests the accuracy of their personal data and we are verifying the accuracy of the data;

(2) the data has been unlawfully processed (ie, in breach of the lawfulness requirement of the first principle) and the individual opposes erasure and requests restriction instead;

(3) we no longer need the personal data but the individual needs us to keep it in order to establish, exercise or defend a legal claim; or

(4) the individual has objected to us processing their data under Article 21(1), and we are considering whether our legitimate grounds override those of the individual.

Note if an individual has challenged the accuracy of their data and asked for us to rectify it under Article 16,

they also have a right to request we restrict processing while we consider their rectification request; or if an individual exercises their right to object under Article 21(1), they also have a right to request we restrict processing while we consider their objection request.

We will not process the restricted data in any way except to store it unless:

- we have the individual's consent;
- it is for the establishment, exercise or defence of legal claims;
- it is for the protection of the rights of another person (natural or legal); or
- it is for reasons of important public interest.

If we have disclosed the information to other organisations we will tell them about the restriction - unless this proves impossible or involves disproportionate effort. If asked to, we will also inform the individual about these recipients.

The 2018 Act defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

The restriction may be lifted when the purpose for the restriction being in place has passed.

In many cases the restriction of processing is only temporary, specifically when the restriction is on the grounds that:

- the individual has disputed the accuracy of the personal data and we are investigating this; or
- the individual has objected to us processing their data on the basis that it is necessary for the performance of a task carried out in the public interest or the purposes of our legitimate interests, and we are considering whether our legitimate grounds override those of the individual.

When a restriction is in place owing to an accuracy dispute or an objection to processing based on public interest or legitimate interests, we may decide to lift it once we have made a decision on the accuracy of the data, or whether our legitimate grounds override those of the individual.

We will inform the individual before we lift the restriction.

We can refuse to comply with a request for restriction if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If we consider that a request is manifestly unfounded or excessive, we can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

And will justify that decision.

We will base the reasonable fee on the administrative costs of complying with the request. If we decide to charge a fee the individual will be contacted without undue delay and within one month. We are entitled not comply with the request until the fee has been received.

5. Objections to Processing

We are required to inform individuals of their right to object "at the point of first communication" and in our privacy notice.

We will consider any objection individuals have that are based on grounds relating to his or her particular situation.

We will 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;
- the processing is for the establishment, exercise or defence of legal claims; or
- the request is manifestly unfounded or excessive. We will not charge a fee to respond in this instance

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

6. Dealing with a Data Breach

When a personal data breach as occurred, we will act in an appropriate and timely manner, and establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we must notify the ICO; if it's unlikely then we don't have to report it. We will document the justification for our decision as to whether or not to notify the ICO.

The data protection officer is to be made aware of suspected breaches immediately.

In assessing risk to rights and freedoms we will focus on the potential negative consequences for individuals including physical, material or non-material damage to natural persons such as

- loss of control over their personal data
- limitation of their rights
- discrimination
- identity theft or fraud
- financial loss
- unauthorised reversal of pseudonymisation
- damage to reputation
- loss of confidentiality of personal data protected by professional secrecy
- or any other significant economic or social disadvantage to the natural person concerned.

We will notify affected data subjects of breaches that affect their rights and freedoms promptly and steps so that they can take steps to protect themselves

Part III – Implementation at Kingsclere Village Club

1. Key People and Information

Data Protection Registration Number	ZA239059	Date of renewal	March annually (auto renews)

Data Protection Officer	S Morris	Chairman@kingsclerevillageclub.co.uk	07576 249814
Data Controller	S Morris	Chairman@kingsclerevillageclub.co.uk	07576 249814
EU representative for Google	S Morris	Chairman@kingsclerevillageclub.co.uk	07576 249814
Information Commissioner's Office	Helpline	0303 123 1113	

2. Our Data Breach Reporting Procedure

Data Protection Breaches are to be reported via Incident Reporting Procedure

To Report an Incident or Dangerous Occurrence:

In an Emergency

If emergency services are required – call 999

Your location is Kingsclere Village Club, 35 George Street, Kingsclere, RG20 5NH

Notify a Trustee as soon as is practicable

Helen Andrew 07887 521359

Emma Hartley 07849 653809

Sharon Morris 07576 249814

In a Non-Emergency

Please notify the booking secretary

Emma Hartley 01635 297913 bookings@kingsclerevillageclub.co.uk

In all Circumstances:

Complete a written report in one of the incident reporting books situated in the kitchen, servery and holding room, and forward your report to the committee via our letter box.

Reports of Data Breach will be forwarded immediately to our Data Protection Office. On receiving a report of a data breach, our response will have four stages

i. Containment and Recovery

Our Data Protection Officer will liaise with the relevant people to stop the breach continuing, investigate what has occurred, recover losses and undertake damage limitation.

ii. Assessment of Ongoing Risk

Some breaches will cause a degree of inconvenience, whereas more serious breaches can lead to harm such as ID theft.

- Factors that will be considered include:
- What type of data is involved?
- How sensitive is it
- Has it been lost, stolen or damaged?
- Is it encrypted?
- What could the data tell a third party about the individual?
- How many individuals' personal data are affected by the breach?
- Who are the individuals whose data has been breached?
- What harm can come to those individuals
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service we provide?
- Do we need advice from an outside agency

iii. Notification of breach

- We must let data subjects affected know about the breach and tell them how to protect themselves, plus decide whether the ICO needs to be notified. Notification must be within 72 hours.
- In line with current guidance, we will notify the ICO if a large number of people are affected, or there are very serious consequences.
- When notifying individuals and others about the breach, the following information will be included:
  - description of how and when the breach occurred and what data was involved;
  - details of what we have already done to respond to the risks posed by the breach
- When notifying individuals we will give specific and clear advice on the steps they can take to protect themselves and also what we are willing to do to help them.

- We will provide a way in which they can contact us for further information or to ask questions about what has occurred.

- When notifying the ICO we will also include details of:
  - security measures in place such as encryption and, where appropriate, details of the security procedures we had in place at the time the breach occurred.
- If the media are aware of the breach so that they can manage any increase in enquiries from the public.
- When informing the media, we will inform them whether we have contacted the ICO and what action is being taken. If the ICO advise us to tell the media, we will follow that advice.

iv. Evaluation and Response

In order to promote good governance and a report will be made and presented to the committee at the next committee meeting. In addition to outlining the specifics of the breach, it will also evaluate our response, and if necessary make recommendations and invite recommendations from the committee.

3. Our Data Audit

Our data audit has identified that that we usually process personal data as part of forming contracts with our users, and that we do not keep that data beyond the term of the contract. The only exceptions being classes where students have not renewed and are sent one reminder ahead of a new term starting; contractors where we may want to undertake works with them at a later date; and contact details for user groups that are published on our website which have been supplied by the user group.

We also process some personal data when fulfilling our constitutional and governance obligations, for instance in minutes of meetings, and on committee nominations. These are kept indefinitely to meet charity law requirements.

Our mailing list is kept entirely separate, and entirely voluntary to subscribe to/unsubscribe from.

We also collect personal data via CCTV, which is collected, stored and accessed in a manner so as to minimise any negative impact of the rights of individuals legitimately using our facility.

A unique feature of the Kingsclere Village Club is that it is a community group, which means the volunteers running the club may have personal data belonging to users of the club on their personal computers and devices; and that there is a small degree of overlap between processing data for personal and village club purposes. For example this overlap may entail ask a personal contact for advice about an issue the Village Club is facing, or thank them for helping with a project. The personal data would never be published, or added to the mailing list without consent.

This audit will be kept under review.

4. Training Needs Analysis

A formal assessment is yet to be undertaken. Many of our Trustees have received training about data protection in their workplace. Not all volunteers process personal data, however we need to establish a baseline of knowledge. Everyone needs to know how our organisation protects data. As such all trustees and admins support need to have knowledge of the principles of data protection, rights of data subjects and how as an organisation we respond to breaches and requests. Regular training to raise awareness on these matters will be provided.

5. Action Plan

	Who is responsible for this plan?	sharon morris						
	What is the main objective?	to ensure the organisation is aware of its responsibilities and is well placed to respond to requests.						
	What is the timescale?	Ongoing						
	Action What steps do you need to take?	**Impact** Why do you need to take this action?	**Priority** High/med/low	**Owner** Who is responsible for this action?	**Start** When will you start?	**End** When are you aiming to finish work on this action?	**Review** to be updated regularly – what have you done so far, and what is causing delay?	**Completed** When did you complete the action?
Procedural – How you handle the requests you receive	Forward requests to the clerk and charman	Establish prompt responses to requests	med	chairman	04/01/2024	ongoing	n/a	n/a
Technical – The tools and resources available to you	Identify factors that slow the reporting of or responses to requests	Establish prompt responses to requests	med	chairman	04/01/2024	ongoing	n/a	n/a
	Ensure staff handling requests correctly store correspondence about each request in a way which allows you to find it and read it easily	It will be easier and quicker to share, collaborate on, and review requests	med	chairman	04/01/2024	ongoing	n/a	n/a
Organisational – How your organisation as a whole can support this plan	Ensure all staff are appropriately trained – use ICO training materials if necessary	Time taken to recognise and refer requests, and to respond to internal consultations will be improved	med	chairman	04/01/2024	ongoing	n/a	n/a
	Have data protection as a regular agenda item at trustee meetings	Promote culture of awareness and openess	med	chairman	04/01/2024	ongoing	n/a	n/a

6. Our Privacy Notices

We have three privacy notices, one relating to the administration of activities, classes, events, markets and such like, another relating to our use of CCTV. Both will be added to the website, and the third relating to our marketing lists.