

Kyle of Sutherland Fisheries (KSF)

(Kyle of Sutherland Fisheries Trust; Kyle of Sutherland District Salmon Fishery Board)



DATA HANDLING POLICY & WEBSITE PRIVACY POLICY

Key Details

Policy prepared by: Jacqui HAMBLIN
Approved by Board: May 2018
Policy became operational on: 25th May 2018
Next Review Date: June 2020

Purpose

The Kyle of Sutherland Fisheries (KSF) has rights and duties under the Salmon and Freshwater Fisheries (Consolidation) (Scotland) Act 2003 and in the pursuance of its charitable objects which include the (protection of fish and their habitats in the KSF district), which necessitates the processing of data.

General Data Protection Regulation (GDPR)

The GDPR 2018 describes how organisations must collect, handle and store personal information.

- Complies with General Data Protection Regulations and follows good practice
- Protects the right of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of data breach

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

1. Data held

The GDPR requires that any information must be under one of six legitimate bases. These are: Public task; Legitimate interests; Contract; Consent; Legal obligation and Vital interests

1.1 Public Task

KSF may process the following data necessary for it to perform its public task with respect to the protection of salmon within its district and the functioning of KSF, which duties are set out within the Salmon Act 2003. This may comprise keeping and maintaining an up to date database which includes names and addresses of:-

- Fishing proprietors within the district
- Mandatories of fishing proprietors
- Persons associated with bailiffing activities
- Other persons or groups with an interest in fisheries in the district that are relevant to the work of the Board
- Other persons or businesses with an interest in fisheries out-with the district that are relevant to the work of the Board

1.2 Legitimate interests

KSF may process data on data subjects that may include persons or businesses with an interest in the work of the KSF in the district but not related directly to its public functions. This may include local fishery interests, local environmental groups and businesses with an interest in fisheries out-with

the district. Data held and processed under legitimate interests will be subject to a 'Legitimate interests Assessment' (LIA).

1.3 Contract

KSF may process data where it is necessary for a contract that KSF has with an individual. KSF will hold the details on file for so long as it has an interest under the contract and no longer than the limitation period for breach of contract, which is 5 years.

1.4 Consent

In cases not covered by Public Task; Legitimate Interests and Contract the Board will seek consent of a person whose data it wishes to hold and set out the purpose for which the information will be processed.

2. Data Handling/Processing

KSF accepts that it is a data controller for the purposes of the GDPR and that it must comply with the following six principles for the handling of personal data:-

- Fairly and lawfully processed
- Processes for limited purposes
- Adequate and relevant and limited to what is necessary
- Accurate and where necessary up to date
- Not kept in a way that people can be identified from it for longer than is necessary
- Processed in a way that ensures appropriate security

3. Data Bases

The KSF officer responsible for the compliance of GDPR is Jacqui Hamblin. She will maintain KSF databases in compliance with GDPR. KSF will hold four separate databases:

- A **Public Task** database of data held necessary to uphold KSF constitution and statutory duties
- A **Contract** database with information required in fulfilment of those contracts
- A **Legitimate Interests** database held subject to satisfaction of a 'legitimate interests assessment' (LIA assessment)
- **Consent** database, all data held under consent of the data subjects

4. Security/Storage

KSF will ensure that its data storage measures are appropriate to the size of KSF network and information systems. KSF will carry out and document an annual audit of the security of its data storage.

These rules describe how and where data should be safely stored. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

When not required, the paper or files should be kept in a locked drawer or filing cabinet. Employees should make sure paper and printouts are not left where unauthorised people could see them. Data print outs should be shredded and disposed of securely when no longer required. When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designation drives and servers. And should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location.
- Data should be backed up frequently. Those backups should be tested regularly, in line with KSF standard back up procedures.
- Data should never be saved directly to mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

5. Audit

KSF will audit its information annually to ensure that its data bases are complaint with the six principle of GDPR. In Particular, the audit will ensure:

- That data is held in compliance with the act
- Data held is accurate
- That no more data is held that is necessary
- That data will be held only for so long as it is needed.

6. Staff Guidelines

The only people able to access data covered by this policy should be those who need it for their work.

- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- KSF will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep data secure by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should not be shared.
- Personal data should not be disclosed to unauthorised people, either within KSF or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager if they are unsure about any aspect of data protection.

7. Subject access rights

All individuals who are subject to personal data held by KSF are entitled to:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to delete;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling

7.1 Subject access requests

An individual may request access to the personal data held by KSF. This request should be made in writing or by email. KSF will always verify the identity of anyone making a subject access request before handing over any information. There is no charge for this and KSF must provide the information within 28 days of the request.

8. Privacy Notice

KSF aims to ensure that individuals are aware that their data is being processed and that they understand:

- KSF contact details
- The purpose for which the information is being held
- How to exercise their rights
- The lawful basis of processing and the period for which the information will be retained.

To these ends, KSF has a privacy statement, setting out how data relating to individuals is used by KSF. The privacy statement is published on KFS website with attention drawn to this in all communications.

Privacy Statement

Here at Kyle of Sutherland Fisheries (KSF) we take individuals privacy seriously. KSF hold certain personal data for the purpose of fulfilling its statutory responsibilities under the Salmon and Freshwater (Consolidation) (Scotland) Act 2003, and fulfilling its charitable objects as set out in its constitution, which includes the protection of salmon fisheries (fish and their habitat) for the public benefit within its district. We do not sell personal data to third parties. We will only pass personal data to third parties without the consent of the data subject where it is necessary for us to do so in support of our statutory responsibilities. Data is held subject to our Data Handling Policy. KSF responsible officer for data is Jacqui Hamblin and any queries regarding this Privacy Statement should be directed to her.

You have rights of access to the personal data held on you and for what purpose it is held and used. You have the right to change your communication preferences at any time.

Kyle of Sutherland Fisheries Trust; Kyle of Sutherland District Salmon Fishery Board, Bank House, Ardgay, Sutherland IV24 3BG. Tel: 01863 766702 Email: admin@kylefisheries.org Web: www.kylefisheries.org

9. DATA COLLECTION & STORAGE PROCESS

Database	Categories	Purpose	Storage	Assessment	Hold period
Public Task	Proprietors & Mandatories Persons associated with bailiffing activity <i>Persons or groups with interest relevant to the work of KSF:-</i> In district e.g SSE; River Workers; Fishfarms Out-with district e.g Other fishery bodies	Membership Communication Conservation Protection & Prevention	Secure Database; Log book	Statute & Constitution	As per policy
Legitimate Interest	<i>Persons or Businesses with interest not related directly with KSF public functions:-</i> In District e.g Angling clubs, Environmental groups Out-with district e.g FMS, AST or other organisations	Registered Interest & Assessment (LIA) Communication	Secure database	LIA tests 1. Purpose 2. Necessity 3 Balancing	As per policy
Contract	Employees Suppliers Customers	Salaries Accounting Communication	Sage Program; Locked cabinet	Contracted	Under contract; Outside contract 5 years
Consent	Persons not covered under Public Task, Legitimate Interest or Contract	Communication	Secure Database	Consent required	Upon request or Change of purpose

Website Privacy Policy

The policy: This privacy policy is for the website: <http://www.kylefisheries.org> and served by Kyle of Sutherland Fisheries, Bank House, Ardgay, Sutherland, IV24 3BG and governs the privacy of its users who choose to use it. It explains how we comply with the GDPR (General Data Protection Regulation), the DPA (Data Protection Act) [pre GDPR enforcement] and the PECR (Privacy and Electronic Communications Regulations).

This policy will explain areas of the website that may affect your privacy and personal details, how we process, collect, manage and store those details and how your rights under the GDPR, DPA & PECR are adhered to. Additionally it will explain the use of cookies or software, advertising or commercial sponsorship from third parties and the download of any documents, files or software made available to you (if any) on this website. Further explanations may be provided for specific pages or features of this website in order to help you understand how we, this website and its third parties (if any) interact with you and your computer / device in order to serve it to you. Our contact information is provided if you have any questions.

Use of Cookies Our website uses cookies to better the users experience while visiting the website. As required by legislation, where applicable this website uses a cookie control system, allowing the user to give explicit permission or to deny the use of /saving of cookies on their computer / device.

What are cookies? Cookies are small files saved to the user's computer's hard drive that track, save and store information about the user's interactions and usage of the website. This allows the website, through its server to provide the users with a tailored experience within this website. Users are advised that if they wish to deny the use and saving of cookies from this website on to their computers hard drive they should take necessary steps within their web browsers security settings to block all cookies from this website and its external serving vendors or use the cookie control system if available upon their first visit. **Website Visitor Tracking** This website uses tracking software, Google Analytics, to monitor its visitors to better understand how they use it. The software will save a cookie to your computer's hard drive in order to track and monitor your engagement and usage of the website, but will not store, save or collect personal information.

Adverts and Sponsored Links The website may contain sponsored links and adverts. These will typically be served through our advertising partners, who may have detailed privacy policies relating directly to the adverts they serve. Clicking on any such adverts will send you to the advertiser's website through a referral program which may use cookies and will track the number of referrals sent from this website. This may include the use of cookies which may in turn be saved on your computer's hard drive. Users should therefore note they click on sponsored external links at their own risk and we cannot be held liable for any damages or implications caused by visiting any external links mentioned.

Downloads & Media Files Any downloadable documents, files or media made available on this website are provided to users at their own risk. While all precautions have been undertaken to ensure only genuine downloads are available users are advised to verify their authenticity using third party antivirus software or similar applications. We accept no responsibility for third party downloads and downloads provided by external third party websites and advise users to verify their authenticity using third party antivirus software or similar applications.

Contact & Communication With us Users contacting this us through this website do so at their own discretion and provide any such personal details requested at their own risk. Your personal information is kept private and stored securely until a time it is no longer required or has no use. Where we have clearly stated and made you aware of the fact, and where you have given your express permission, we may use your details to send you products/services information through a mailing list system. This is done in accordance with the regulations named in 'The policy' above. **Email Mailing List & Marketing Messages** We will only contact you if you specifically agree to receiving information. We will never add your information to a mailing list without your express permission.

External Website Links & Third Parties Although we only look to include quality, safe and relevant external links, users are advised to adopt a policy of caution before clicking any external web links mentioned throughout this website. Shortened URL's; URL shortening is a technique used on the web to shorten URL's (Uniform Resource Locators) to something substantially shorter. This technique is especially used in social media and looks similar to this (example: <http://bit.ly/zyVUBo>). Users should take caution before clicking on shortened URL links and verify their authenticity before proceeding. We cannot guarantee or verify the contents of any externally linked website despite our best efforts. Users should therefore note they click on external links at their own risk and we cannot be held liable for any damages or implications caused by visiting any external links mentioned.

Social Media Policy & Usage We adopt a Social Media Policy to ensure our business and our staff conducts themselves accordingly online. While we may have official profiles on social media platforms users are advised to verify authenticity of such profiles before engaging with, or sharing information with such profiles. We will never ask for user passwords or personal details on social media platforms. Users are advised to conduct themselves appropriately when engaging with us on social media. There may be instances where our website features social sharing buttons, which help share web content directly from web pages to the respective social media platforms. You use social sharing buttons at your own discretion and accept that doing so may publish content to your social media profile feed or page.