Kings Hill Parish Council

Action Plan – GDPR – January 2021

No.	Action Required	By Whom	By When	Comp-lete?
	CCTV Policy			
1.	Confirm that all members are aware of the restrictions in relation to access to, and disclosure of recorded images.			
2.	Parish Council members and staff will have access to details of where CCTV cameras are situated, with the exception of cameras place for the purpose of covert monitoring. Do a map and place of website.			
3.	The Parish Council complies with the Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its use.			
4.	CCTV has the potential to be privacy intrusive. The Parish Council will perform a privacy impact assessment when installing or moving CCTV cameras to consider the privacy issues involved with using new surveillance systems to ensure that the use is necessary and proportionate and address a pressing need identified – undertake privacy impact assessment for all the CCTV cameras.			
5.	The Parish Council's CCTV is registered with the Information Commissioner under the requirements of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) 2016/679 - Check			
6.	It is a requirement of the Data Protection Act to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The Parish Council is to ensure that this requirement is fulfilled. The CCTV sign should include the following: • That the area is covered by CCTV surveillance and pictures are recorded. • The purposes of using CCTV.			

No.	Action Required	By Whom	By When	Comp-lete?
	• The name of the Parish Council. • The contact telephone number or address for enquiries.			
	Data Protection Policy			
7.	All individuals permitted to access personal data in line with their work duties must agree to comply with this policy and agree to undertake any relevant training that may be appropriate to the role being undertaken. Train staff and members and obtain signature to state they have received the training and understand?			
8.	The Data Protection Officer will provide an annual report of their activities and, where relevant, report to the committee their advice and recommendations on Parish Council data protection issues. Action for note in May to ask for report for May AGM			
9.	External agencies or companies contracted to undertake processing of personal data on behalf of the Parish Council must demonstrate, via a written agreement, that personal information belonging to the Parish Council will be handled in compliance with the GDPR and DPA and that it has the necessary technical and organisational security measures in place to ensure this. • IT • Data Protection Officer • Rilatus			
10.	The Parish Council will use a Data Protection Impact Assessment (DPIA) toolkit to evaluate all new computer systems to help it determine how data protection compliance can be assured. In addition, all existing systems will be subject to periodic assessment.			
11.	The Parish Council have implemented a process to ensure all staff handling personal information know when and how to report any actual or suspected data breach(es), and that appropriately trained staff manage these breaches correctly, lawfully and in a timely manner. Sports Park internal training – laminated card.			
12.	Staff and Member training annually.			

No.	Action Required	By Whom	By When	Comp-lete?
	Freedom of Information Policy			
13.	Methods of handling information are regularly assessed and evaluated; How – My Audit on handling of data.			
14.	Any contractual information, or information obtained from organisations during the tendering process, held by the Parish Council are subject to the provisions of the FOIA and EIR. Whenever the Parish Council enters into contracts, it will seek to exclude contractual terms forbidding the disclosure of information beyond the restrictions contained in the legislation. A standard form of wording will be included in contracts to cover the impact of FOIA and EIR in relation to the provision of information held in contracts.			
15.	The Parish Council shall make a disclosure log available on the Parish Council website that sets out responses to previous FOI requests.			
	Subject Access Request Procedure			
16.	Copy of disclosed documents to be kept on a secure system.			
	Security Incident and Data Breach Policy			
17.	This policy applies to all information held by the Parish Council falling within the scope of the General Data Protection Regulation and Data Protection Act 2018, in all formats including paper, electronic, audio, and visual. It applies to all staff and those working on behalf of the Parish Council who have access to Parish Council information. This policy takes effect immediately and all staff should be made aware of security incident requirements. Any queries should be directed to the Clerk and Responsible Officer (contact details below). Training and signed to say understood.			
18.	Breach Management Plan The Clerk and Responsible Officer will lead all data breach investigations and will follow			

No.	Action Required	By Whom	By When	Comp-lete?
	the Information Commissioner's Office (ICO) suggested Breach Management Plan:- 1. Containment and Recovery 2. Assessment of ongoing risk 3. Notification of Breach 4. Evaluation and Response			
19.	The Clerk and Responsible Officer will decide whether the Information Commissioner's Office (ICO) or the data subjects should be notified of the breach and will inform the Chair. The ICO must be notified within 24 – 72 hours. This is the sole responsibility of the Clerk and Responsible Officer and staff must not make any notifications directly.			
20.	Keep a breach log.			
	Information Security Policy			
21.	All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by IT Consultant or by such third party/parties as the Chair and Committee members may authorise. How do you want to word this?			
22.	Business continuity and disaster recovery plans for all critical activities will be produced, tested and maintained – review			
23.	The Parish Council secure the buildings at certain times to prevent unauthorised access to the buildings. An alarm system is set nightly. Is this correct?			
24.	Training in this policy?			
25.	You are not entitled to install any software of your own without the approval of the Clerk and Responsible Officer. Any software belonging to you must be approved by the Clerk and Responsible Officer and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject. Prior to installation of any software onto the IT Systems, you must obtain written permission by the Clerk and			

No.	Action Required	By Whom	By When	Comp-lete?
	Responsible Officer. This permission must clearly state which software you may install, and onto which computer(s) or device(s) it may be installed. Is there any non work related software on computers, should we backdate for Rialtus etc?			
26.	Physical media (e.g. USB memory sticks or disks of any kind) may not be used for transferring files. The Clerk and Responsible Officer's approval must be obtained prior to transferring of files using cloud storage systems. Are there any USB sticks in operation.			
27.	All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the Clerk and Responsible Officer. Biometric log-in methods can only be used if approved by the Clerk and Responsible Officer. Are we doing this?			
28.	Personal or confidential information should not be removed from the Parish Council without prior permission from the Clerk and Responsible Officer except where the removal is temporary and necessary. When such permission is given you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained. To note.			
29.	You must ensure that the information is: a) not transported in see-through or other un-secured bags or cases; Let staff know to use envelopes and not the see through plastic covers.			
	Information Sharing Policy			
30.	All ISA's should be drafted using the Parish Council's standard Information Sharing Agreement Template (Appendix 1). The Clerk and Responsible Officer should be consulted when it is believed an ISA is required. You must ensure when entering into any regular information sharing arrangements that an Information Sharing Agreement is in place and that it states a clear and lawful legal basis to allow the sharing to take place and it is agreed by all parties and approved by the Clerk and Responsible Officer.			

No.	Action Required	By Whom	By When	Comp-lete?
	All information sharing agreements must be regularly reviewed and will be stored centrally by the Parish Council and published on the Parish Council's website.			
31.	To undertake a data held exercise.			
	Forms			
32.	CC and SP Booking Forms			
33.	Allotment waiting list forms			