Adastra Hall Hassocks Community Association

Data Protection Policy and Procedure

Adastra Hall Hassocks Community Association (AHHCA) is responsible for all aspects of the management of Adastra Hall. It is run by Trustees and volunteers and contracts a booking secretary and cleaners.

The AHHCA seeks to be compliant with all aspects of the General Data Protection Regulations. The lawful basis on which information is kept by HCA is "in pursuit of the organisations legitimate interests", or "Legitimate interests". This includes personal data for the purposes of running the affairs of the Hall.

Personal Data includes anything that can identify an individual, including (but not exclusively) names, addresses, email addresses, phone numbers, age, employment history, photographs. There is no cctv footage.

AHHCA has no reason and will not collect and hold information that falls into 'special categories' defined as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data about a person's sex life or sexual orientation". For this reason consent to hold the information we keep is not required.

The following Privacy Notice will be used on all documentation requiring personal information eg hirers agreement, emails.

"Adastra Hall Hassocks Community Association uses personal data for the purposes of managing Adastra Hall, its booking and finances, running and marketing events at the Hall, staff employment and its fundraising activities. Data maybe retained for up to 7 years for accounts purposes and for longer where required, eg by the Hall's insurers. If you would like to see our Data Protection Policy please ask for a copy."

Personal Data (PD) is collected and processed with due consideration of 8 basic principles

1. it is processed fairly, lawfully and in a transparent manner
2. it is collected only for the specified lawful purposes and not used for anything else
3. it should be adequate relevant and not excessive for the purpose
4. it shall be accurate and where appropriate kept up to date
5. it shall not be kept for longer than the purpose for which it was collected

6. it will be processed within the lawful rights of the data subject

7. measures will be taken to protect data against unlawful use, loss, destruction or damage

8. it will not be transferred to any other country that does not have adequate protections

Policy - all trustees, committee members and volunteers will understand what constitutes PD, how HCA handles it, the legitimate uses of it and what to do if they are aware of a data breach.

Procedure - all new recruits will need to handle some PD, no matter how little, and will be shown this policy, given the opportunity to clarify understanding and asked to sign that they understand it. It is inevitable that some individual data, names, email and phone numbers will be held for HCA purposes and also private use, i.e. the worker and the hirer are friends. In this instance the advice will be to only keep essential PD and treat the information in the same way that they would like their information to be treated.

Policy - all PD will be held in a secure way, with measures taken to ensure that information is not accidentally shared.

Procedure - electronic devices of all kinds will be password protected such that only the committee member can access it. All such data will be appropriately backed up. Committee member and volunteers will only keep such data as they actually need, deleting it when no longer required.

Policy - the Trustees will identify a Data Protection Contact to oversee the use of PD. They will be expected to familiarise themselves with this policy and relevant documentation, know where to look for advice, be the point of contact for any concerns regarding data breaches and make sure that the committee keeps data protection in mind for every policy change and hall development.

Procedure - the committee will nominate and approve a Trustee for this function at the first meeting after the adoption of this policy, and ensure that in the event of that individual no longer being active, ensure a prompt replacement.

Policy - the Trustees will know where all PD is located and ensure appropriate security measures are in place.

Procedure - a 'map' will be maintained by the secretary, reviewed when any new storage system is utilised and at least annually, of where all PD is kept. This will include paper filing of documents, use of electronically held data on mobile phones, laptops and PC's, tablets, memory sticks and external hard drives etc. All paper files with PD will be kept in the locked office where possible, with only minimal documents kept safely at home by the Treasurer, Booking Secretary or Secretary. All electronic devices used by committee members will have password protection that is accessible only to them. Any trustee, committee member or volunteer will be asked to confirm that they have deleted any PD from all their devices, and returned any paper documents to the office to be processed appropriately. Original documents of special importance, such as the lease and minute archive, shall be kept very securely by Hassocks Parish Council, with HCA keeping copies securely.

Policy - use of photographs with identifiable people in, eg for illustration purposes on the website or other promotional material by the committee, will be treated as PD.

Procedure - photos will only be used if the adults within have given their permission. If an event is to be photographed in full swing, an announcement should be made of the intention to take a photo and the use it is to be put to, inviting those who do not wish to be in it to step aside. No photo with identifiable children in it will be taken or published without the written consent of a parent or legal guardian only.

Policy - all data breaches will be treated very seriously and in compliance with the General Data Protection Regulations.

Procedure - a data breach is a breach of security that leads to the destruction, alteration, loss, unauthorised disclosure of or access to, PD. This could include the accidental copying of an email to a list of people that had no need to see each others email addresses. All staff are advised to take extra care when emailing that the bcc (blind carbon copy) option should be used rather than cc when there is no requirement to share addresses. All workers will be mindful of protecting PD at home by not leaving it where others could see it. If a breach is feared the Data Protection Contact should be immediately be contacted and action taken as appropriate. In some circumstances, where it is deemed that there may be a loss to individuals, a breach must be reported to the Information Commissioners Office (ICO). If in doubt, this can be checked with the ICO on the phone, details on their website. The Data Protection Contact must keep the trustees promptly updated. All breaches must be reported to the committee and discussed at the next meeting as an incident.

Policy - the AHHCA will respond to all Subject Access Requests (SAR) in line with GDPR. Anyone who believes that the AHHCA holds PD on them, has the right to see it, to know how it is stored and used, and to challenge and change anything that is incorrect.

Procedure - any committee member or volunteer who receives a request from an individual regarding their own data, should be directed to the Data Protection Contact. The request should be responded to within 30 days of being seen in writing. The DPC will remind themselves of the policy and seek advice as necessary, before checking the identity of the person making the request which is likely to involve photo-id, as to give out PD to the wrong person is a further breach. As many requests to see PD are the result of a complaint, HCA will ensure that its complaints policy and procedure is fit for purpose and followed effectively.

Policy - the AHHCA recognises that the business of the Hall changes over time and will ensure that its responsibilities regarding DP are regularly reviewed and adapted as necessary.

Procedure - the committee will hold in mind the implications for DP of any new storage method, activity, website development, policy, contract to manage personal data (eg new booking system, mailing list management etc). This policy will be reviewed at least annually, with particular reference to

- whether we need to to appoint a Data Protection Officer, and any justification for not.

- keeping our data map up to date

- whether any of our data collected requires consent