Crockenhill Village Hall
Registered charity: 302724

CROCKENHILL VILLAGE HALL MANAGEMENT COMMITTEE (CVHMC)
GENERAL DATA PROTECTION REGULATION (GDPR) Policy Operational Guidelines

Operational Guidance

Email: All trustees, staff and volunteers should consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained it should be saved into the appropriate folder or printed and stored securely.

NB: emails that contain personal information no longer required for operational use, should be deleted from the personal mailbox and any "deleted items" box.

Phone Calls: Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

Personal information should not be given out over the telephone unless you have no doubts as to the caller's identity and the information requested is innocuous.

If you have any doubts, ask the caller to put their enquiry in writing.

If you receive a phone call asking for personal information to be checked or confirmed be aware that the call may come from someone impersonating someone with a right of access.

Laptops and Portable Devices: All laptops and portable devices that hold data containing personal information must be protected with a suitable encryption program (password).

Whenever possible ensure your laptop is locked (password protected) when left unattended, even for short periods of time.

Whenever possible ensure when travelling in a car, that the laptop is out of sight, preferably in the boot.

If you have to leave your laptop in an unattended vehicle at any time, whenever possible put it in the boot and ensure all doors are locked and any alarm set.

Never leave laptops or portable devices in your vehicle overnight.

Do not leave laptops or portable devices unattended in restaurants or bars, or any other venue.

When travelling on public transport, keep your laptop or portable device with you at all times, do not leave it in luggage racks or even on the floor alongside you.

Data Security and Storage: Store as little personal data as possible on your computer or laptop; only keep those files that are essential. Personal data received on disk or memory stick should be saved to the relevant file on the server or laptop. The disk or memory stick should then be securely returned (if applicable), safely stored or wiped and securely disposed of.

Remember to lock (password protect) your computer or laptop when left unattended, particularly in public places.

Passwords: Do not use passwords that are easy to guess. All your passwords should contain both upper and lower-case letters and preferably contain some numbers. Ideally passwords should be 6 characters or more in length.

Protect Your Password:

Common sense rules for passwords are: do not give out your password

Do not write your password somewhere on your laptop

Do not keep it written on something stored in the laptop case.

Data Storage: Personal data will be stored securely and will only be accessible to authorised volunteers or staff.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately. For financial records this will be up to 7 years. For employee records see below. Archival material such as minutes and legal documents will be stored indefinitely. Other correspondence and emails will be disposed of when no longer required or when trustees, staff or volunteers retire.

All personal data held for the organisation must be non-recoverable from any computer which has been passed on/sold to a third party.

Information Regarding Employees or Former Employees: Information regarding an employee or a former employee, will be kept indefinitely. If something occurs years later it might be necessary to refer back to a job application or other document to check what was disclosed earlier, in order that trustees comply with their obligations e.g. regarding employment law, taxation, pensions or insurance.

Accident Book: This will be checked regularly. Any page which has been completed will be removed, appropriate action taken and the page filed securely.

Data Subject Access Requests: CVHMC may occasionally need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies in circumstances which are not in furtherance of the management of the charity. The circumstances where the law allows the charity to disclose data (including sensitive data) without the data subject's consent are:

a) Carrying out a legal duty or as authorised by the Secretary of State Protecting vital interests of a Data Subject or other person e.g. child protection

b) The Data Subject has already made the information public

c) Conducting any legal proceedings, obtaining legal advice or defending any legal rights

d) Monitoring for equal opportunities purposes – i.e. race, disability or religion

CVHMC regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom it deals.

CVHMC intend to ensure that personal information is treated lawfully and correctly.

Risk Management: The consequences of breaching Data Protection can cause harm or distress to service users if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Trustees, staff and volunteers are made aware that they can be personally liable if they use customers' personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of the charity is not damaged through inappropriate or unauthorised access and sharing.