



Hale Community Centre

Privacy/Data Protection Policy & Procedures

INTRODUCTION

Who we are: Hale Community Centre, registered in England as a charity (Charity No. 1132822) and as a charitable company limited (company number 06872992).

Contact Details: Any questions regarding this Policy or our privacy practices should be sent to the Centre Manager by email – manager@halecommunitycentre.org.uk or by writing to:

Hale Community Centre, 130 Upper Hale Road, Farnham Surrey GU9 0JH

We are committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of Personal Data (PERSONAL DATA) in order to carry on our work of managing Hale Community Centre. This personal information must be collected and handled securely.

The **Data Protection Act 1998 (DPA)** and **General Data Protection Regulations (GDPR)** govern the use of information about people (personal data). Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographs.

The charity will remain the data controller for the information held. The trustees, staff, consultants, contractors or volunteers are personally responsible for processing and using personal information in accordance with the Data Protection Act and GDPR. Trustees, staff, consultants, contractors and volunteers who have access to personal information will therefore be expected to read and comply with this policy.

PURPOSE

The purpose of this policy is to set out the Hale Community Centre's commitment and procedures for protecting personal data. Trustees regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal with. We recognise the risks to individuals of identity theft and financial loss if personal data is lost or stolen.

The following are definitions of the terms used:

- *Data Controller* - the trustees who collectively decide what personal information Hale Community Centre will hold and how it will be held or used.
- *Act means the Data Protection Act 1998 and General Data Protection Regulations* - the legislation that requires responsible behaviour by those using personal information
- *Data Protection Officer* – the person responsible for ensuring that Hale Community Centre follows its data protection policy and follows the Act is the Centre Manager.

- *Data Subject* – the individual whose personal information is being held or processed by Hale Community Centre for example a donor or hirer.
- *'Explicit' consent* – is a freely given, specific agreement by a Data Subject to the processing of personal information about her/him.

Explicit consent is needed for processing “sensitive data”, which includes:

- a) Racial or ethnic origin of the data subject
 - b) Political opinions
 - c) Religious beliefs or other beliefs of a similar nature
 - d) Trade union membership
 - e) Physical or mental health or condition
 - f) Sexual orientation
 - g) Criminal record
 - h) Proceedings for any offence committed or alleged to have been committed
- *Information Commissioner's Office (ICO)* - the ICO manages implementing and overseeing the Data Protection Act 1998.
 - *Processing* – means collecting, amending, handling, storing, or disclosing personal information
 - *Personal Information* – information about living individuals that enables them to be identified – e.g., names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers.

THE DATA PROTECTION ACT contains 8 principles for processing personal data with which we must comply - **Lawfulness, fairness, and transparency;** ▪ **Purpose limitation;** ▪ **Data minimisation;** ▪ **Accuracy;** ▪ **Storage limitation;** ▪ **Integrity and confidentiality;** and ▪ **Accountability.**

PERSONAL DATA:

- 1) shall be processed fairly and lawfully and, shall not be processed unless specific conditions are met,
- 2) shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
- 3) shall be adequate, relevant, and not excessive in relation to those purpose(s),
- 4) shall be accurate and, where necessary, kept up to date,
- 5) shall not be kept for longer than is necessary,
- 6) shall be processed following the rights of data subjects under the Act,

- 7) shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,
- 8) shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

APPLYING THE DATA PROTECTION ACT WITHIN THE CHARITY:

We will let people know why we are collecting their data, which is for the lawful purpose of managing Hale Community Centre, its hiring, marketing, publicity for events, fundraising and finances. It is our responsibility to ensure personal data is only used for this purpose unless specific consent is given, or the personal data is already in the public domain. Access to personal information will be limited to trustees, staff, consultants, contractors and volunteers.

Where individuals need to be identified in public documents e.g., minutes and where harm may result, initials rather than full names will normally be used.

CORRECTING DATA:

Individuals have a right to make a Subject Access Request (SAR) to find out whether the charity holds their personal data, where, what it is used for and to have data corrected if it is wrong, to prevent use which is causing them damage or distress, or to stop marketing information being sent to them.

Any Subject Access Request (SAR) must be dealt with within 30 days. Steps must first be taken to confirm the identity of the individual before providing information, requiring both photo identification e.g., passport and confirmation of address e.g., recent utility bill, bank or credit card statement.

Any concerns about complying with a Subject Access Request (SAR) need to be discussed promptly with the Centre Manager or with the ICO, e.g., if it is manifestly unfactual or excessive.

RESPONSIBILITIES:

Hale Community Centre is the Data Controller under the Act, and is legally responsible for complying with the Act, which means that it determines what purposes personal information held will be used for.

The Board of Trustees will consider legal requirements and ensure that it is properly implemented, and will through appropriate management and strict application of criteria and controls:

- 1) Collect and use information fairly.
- 2) Specify the purposes for which information is used
- 3) Collect and process proper information, and only to the extent that it is needed to fulfil its operational needs or to follow any legal requirements.

- 4) Ensure the quality of information used.
- 5) Ensure the rights of people about whom information is held, can be exercised under the Act. These include:
 - a) the right to be informed that processing is undertaken.
 - b) the right of access to one's personal information.
 - c) the right to prevent processing in certain circumstances, and
 - d) the right to correct, rectify, block, or erase information which is regarded as incorrect information.
 - e) take appropriate technical and organisational security measures to safeguard personal information,
 - f) ensure that personal information is not transferred abroad without suitable safeguards,
 - g) treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation, or ethnicity when dealing with requests for information,
 - h) set out clear procedures for responding to requests for information

All trustees, staff, consultants, contractors and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them.

The Centre Manager will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

- a) Everyone processing personal information understands that they are contractually responsible for following good data protection practice;
- b) Everyone processing personal information is appropriately trained to do so;
- c) Everyone processing personal information is appropriately supervised;
- d) Anybody wanting to make enquiries about managing personal information knows what to do;
- e) Dealing promptly and courteously with any enquiries about managing personal information;
- f) Describe clearly how the charity manages personal information;
- g) Will regularly review and audit the ways it holds, manages, and uses personal information;
- h) Will regularly assess and evaluate its methods and performance in relation to managing personal information.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998

In case of any queries or questions in relation to this policy please contact the Centre Manager.

PROCEDURES FOR HANDLING DATA & DATA SECURITY

Hale Community Centre has a duty to ensure that appropriate technical, organisational measures and training are undertaken to prevent:

- Unauthorised and unlawful processing of personal data;
- Unauthorised disclosure of personal data;
- Accidental loss of personal data.

All trustees, staff, consultants, contractors and volunteers must therefore ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper, in a computer or recorded by some other means e.g., tablet or mobile phone.

Personal data relates to data of living individuals who can be identified from that data and use of that data could cause an individual damage or distress. This does not mean that mentioning someone's name in a document comprises personal data; however, combining various data elements such as a person's name and salary or religious beliefs etc. would be classed as personal data, and falls within the scope of the DPA. It is therefore important that all staff, consultants and contractors consider any information (which is not otherwise in the public domain) that can be used to identify an individual as personal data and observe the guidance given below

PRIVACY NOTICE & CONSENT POLICY

The Hale Community Centre Privacy Notice is as follows:

'At Hale Community Centre we are committed to protecting personal information and we take our responsibilities regarding the security of personal data very seriously.

Hale Community Centre uses personal data for the purposes of managing the Community Centre, its bookings and finances, fundraising, running and marketing events at the Community Centre, staff employment and its fundraising activities. Data may be retained for up to 7 years for accounts purposes and for longer where required e.g., by the Community Centre's insurers.

Hale Community Centre is the data controller, and we are responsible for your personal data as defined in the Centre's [Privacy/Data Protection Policy & Procedures dated October 2023](#)'.

OPERATIONAL GUIDANCE

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

Emails that contain PERSONAL DATA personal information no longer required for operational use, should be deleted from the personal mailbox and any “deleted items” box.

Where someone not a trustee, employee or contractor needs to be copied into an email e.g., a wider circulation list for an upcoming event, we encourage use of bcc instead of cc, so as to avoid their PERSONAL DATA being shared through forwarding

3. **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.
4. **Laptops and Portable Devices:** All laptops and portable devices that hold data holding personal information must be protected with a suitable password which is changed regularly. Where sensitive data or financial information is held an encryption program should be used.
 - Ensure your laptop is locked (password protected) when left unattended, even for short periods of time.
 - When travelling in a car, make sure the laptop is out of sight, preferably in the boot.
 - If you have to leave your laptop in an unattended vehicle at any time, 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.
 - When travelling on public transport, always keep it with you, do not leave it in luggage racks or even on the floor alongside you.
 - Do not leave laptops or portable devices unattended in restaurants or bars, or any other venue.
5. **Data Security and Storage:** Store as little personal data as possible relating to Hale Community Centre 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.

6. **Wi-Fi Service:** When using the Hale Community Centre's Wi-Fi service, you always agree to be bound by the following provisions:
- 1) not to use the Hale Community Centre Wi-Fi service for any for the following purposes:
 - a) disseminating any unlawful, harassing, libelous, abusive, threatening, harmful, vulgar, obscene, or otherwise objectionable material or otherwise breaching any laws;
 - b) transmitting material that constitutes a criminal offence or encourages conduct that constitutes a criminal offence, results in civil liability, or otherwise breaches any applicable laws, regulations, or code of practice;
 - c) interfering with any other person's use or enjoyment of the Wi-Fi service; or
 - d) making, transmitting, or storing electronic copies of material protected by copyright without permission of the owner;
 - 2) to keep any username, password, or any other information which forms part of the Hale Community Centre's Wi-Fi service security procedure confidential and not to show it to any third party.
6. **Passwords:** Do not use passwords that are easy to guess. Passwords should have both upper and lower-case letters and preferably have some numbers. Ideally passwords should be six characters or more in length. Protect Your Password; common sense rules 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.
7. **Data Storage:** Personal data will be stored securely and will only be accessible to authorised staff, consultants, contractors, or volunteers.
- 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, consultants, contractors 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.
8. **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 to a job application or other document to check what was disclosed earlier, in order that trustees follow their obligations e.g., regarding employment law, taxation, pensions or insurance.
9. **Accident Book:** This will be checked regularly. Any page which has been completed will be removed, action taken, and the page filed securely.

Hale Community Centre may use general photographs of events with groups of adults at the hall for publicity purposes in accordance with its lawful basis for using PERSONAL DATA. Photos of children must not be used without the written consent of the parent or guardian. However, Hale Community Centre is aware that for some individuals publicising their location could place them or their families at risk. Consequently at large events at which publicity photos may be taken a notice should be posted at the entrance, or an announcement made, providing opportunity for people to refuse taking part in publicity photographs. At small events the consent of individuals (verbal) should be obtained if their image will be clearly identifiable. Hirers are encouraged to comply with this policy.

10. Data Subject Access Requests: We 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.

We regard the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal. If an agency asks for personal data not in compliance with one of the above e.g., to obtain information about improving a service a consent form will need to be issued to the data subjects asking for their consent to pass their personal data on

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

11. 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, consultants, contractors, or volunteers should be 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.