Laverstoke and Freefolk Parish Council

POLICIES

19 May 2026

Contents

1. Definitions and Terms

The following definitions applies:

- *Council:* Laverstoke and Freefolk Parish Council.
- *Council Members;* Councillors and staff of the Council.
- *Community Site:* The buildings and land leased from Portals Property Limited.

2. Governance and Review

2.1. Governing Documents

The Council Governing Documents are:

- Standing Orders
- Financial Regulations
- Code of Conduct
- Policies

2.2. Approval of Policies

The Laverstoke and Freefolk Parish Council has reviewed and approved policies in this document on 19 May 2026.

2.3. Review of Governing Documents

The Councils Governing Documents are reviewed by the Council in May in year and when any major change in legislation, activity of the Council or significant incident or event occurs.

3. Information Technology (IT) Policy

3.1. Purpose

This Policy sets out how the Council manages, secures, and uses information technology, digital systems, and data.
Its purpose is to ensure:

- Compliance with AGAR Assertion 10 (Digital & Data Compliance);
- Compliance with data protection legislation (UK GDPR & Data Protection Act 2018);
- Security and integrity of Council-owned information;
- Clear guidance for Council Members, volunteers and contractors.

This policy applies to:

- Council Members; and
- Any volunteers or third parties handling Council data.

3.2. Council-Owned Domain, Email & Digital Accounts

The Council uses a domain that it owns and controls: *laverstokeandfreefolk.org.uk*

3.2.1. Email Accounts

- All Council business must be conducted through Council-issued email accounts;
- Personal email accounts must not be used for Council business;
- Access to Council email accounts must be protected by strong passwords and Multi-factor authentication (MFA), where available.

3.2.2. Account Control

- Accounts are created, monitored and disabled by the Clerk (or delegated IT contractor);
- When a Council Member leaves their Council email account is closed and data is transferred to the Clerk where appropriate.

3.3. Devices and Equipment

3.3.1. Council-Owned Devices

Where the Council issues IT equipment (laptops, tablets, phones), the following applies:

- Devices must only be used for Council business;
- Devices must be password-protected;
- Devices must be kept updated with security patches;
- Antivirus or equivalent protection must be active.

3.4. Personal Devices (BYOD

If personal devices are used for Council business:

- They must be password-protected;
- They must have up-to-date security updates;
- Council data must be stored only in Council-approved applications (e.g., Council email, Council-managed cloud storage);
- If a device is lost or stolen, it must be reported immediately to the Clerk.

The Council reserves the right to require the secure deletion of Council data from personal devices when necessary.

3.5. Data Storage, Access & Backup

3.5.1. Storage Locations

Council data must be stored:

- On Council-managed cloud storage: Council One Drive;
- On Council-owned devices where appropriate;
- Paper records must be held securely.

Data **must not** be stored on:

- Unencrypted USB sticks;
- Personal cloud accounts;
- Social media accounts (other than public postings).

3.6. File Access

- Access to shared drives is authorised by the Clerk;
- Shared drives must follow a clear folder structure.

3.7. Backups

Backup arrangements:

- Cloud-based systems with automatic backup.

3.8. Data Protection & GDPR

The Council collects and processes personal data to fulfil its duties and obligations as a public authority. The Council is committed to complying with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, ensuring that all personal data is handled lawfully, fairly, and transparently.

All Council Members and volunteers must comply with the *Data Protection Policy*:

3.9. Website & Accessibility

The Council website must:

- Publish transparency and financial information as required by law;
- Comply with WCAG 2.2 AA accessibility standards;
- Publish a valid, reviewed Accessibility Statement;
- Accessibility checks must be carried out at least annually.

3.10. Security Requirements

3.10.1. Passwords

- Must be strong and not reused across services;
- Should be changed if a breach is suspected;
- Must not be shared.

3.10.2. Updates & Patching

- Devices and software must be updated promptly;
- Unsupported software must not be used.

3.11. Network Security

- Public Wi-Fi should be avoided when accessing sensitive information unless a secure connection is used.

3.12. Incident Reporting & Data Breaches

Any of the following must be reported immediately to the Clerk;

- Lost or stolen devices;
- Suspected hacking or phishing;
- Accidental sharing of personal data;
- Website or email security issues;

Data breaches must be logged and managed in accordance with the *Data Breach Policy*.

3.13. Leaving the Council

When a Councillor or staff member leaves:

- Access to Council email and digital services is removed;
- Any Council data on personal devices must be deleted;
- Council-owned devices must be returned;
- Handover of files or information must be completed.

4. Data Protection Policy

4.1. Purpose of This Policy

This policy sets out how the Council manages personal data, explains the rights of individuals, and outlines the responsibilities of staff, Councillors, and volunteers who process personal data on behalf of the Council.

4.2. Data Protection Principles

The Council will ensure that personal data is:

- Processed lawfully, fairly, and transparently;
- Collected for specified, explicit, and legitimate purposes;
- Adequate, relevant, and limited to what is necessary;
- Accurate and kept up to date;
- Kept for no longer than necessary;
- Processed securely.

The Council is responsible for demonstrating compliance with these principles.

4.3. Lawful Bases for Processing

The Council will only process personal data where a lawful basis applies, including:

- Performing a task in the public interest or in the exercise of official authority;
- Compliance with a legal obligation;
- Performance of a contract;
- Consent (only where appropriate and freely given);
- Protection of vital interests;
- Legitimate interests.

Special category data will only be processed under the additional conditions set out in the UK GDPR.

4.4. Roles and Responsibilities

- The Council: overall responsibility for compliance and oversight
- The Clerk: ensures day-to-day compliance, maintains records, manages data subject requests, and reports any personal data breaches
- Council Members, and volunteers: must follow this policy, complete training where required, and report any concerns or breaches immediately

4.5. Types of Personal Data Held

The Council may process personal data including

- Contact details (name, address, phone, email);
- Financial information (for payments, salaries, or grants);
- Employee and Councillor information;
- Correspondence, complaints, and enquiries;
- E-Newsletter subscription (name, email, subscription preferences);
- Planning and licensing consultation responses;
- Data used for management of Community Site;

The Council will only collect data necessary for its functions.

4.6. Data Subject Rights

Individuals have the following rights:

- To be informed about data held;
- To access their data;
- To rectification;
- To erasure (where applicable);
- To restrict processing;
- To data portability (rarely applicable to Councils);
- To object to the holding of data.

Requests should be submitted to the Clerk and will be handled within one month unless an extension is legally permitted.

4.7. Retention and Disposal of Data

- Data will be kept only for as long as necessary, in line with recognised local government retention schedules;
- Secure disposal methods will be applied, including shredding, secure digital deletion, and destruction of storage media when no longer required.

4.8. Data Security

See *IT Policy*.

4.9. Sharing Personal Data

Personal data will only be shared where:

- Required by law
- Necessary for delivering Council services
- Explicit consent has been provided
- Required by external audit or public inspection regulations

Data will not be sold or shared for marketing purposes.

4.10. Data Breaches

See *Data Breach Policy*.

4.11. Privacy Notice

The Council will publish the Privacy Notice on its website.

4.12. Training and Awareness

Councillors, staff, and volunteers involved in handling personal data will receive appropriate guidance and training to ensure compliance with this policy.

5. Data Retention Policy

5.1. Purpose

The purpose of this policy is to ensure that information is retained only for as long as necessary, kept securely, and disposed of appropriately.

5.2. Scope

This policy applies to all information created, received, or maintained by the Council, including:

- Paper records;
- Digital files;
- Emails;
- Photographs, video, and audio;
- Data held by third-party processors;
- Website data and logs.

It covers Council Members, volunteers, contractors, and data processors acting on the Council's behalf.

5.3. Responsibilities

Council (Data Controller): determines what information is held, how long it is retained, and how it is used.
Clerk: responsible for implementing this policy, managing records, and ensuring compliance
Councillors: must follow this policy and ensure personal data is only kept as long as required
Data Processors (e.g., website host & email provider): must follow the Council's retention and disposal instructions.

5.4. Legal and Regulatory Framework

Retention periods are based on statutory requirements and best-practice guidelines, including:

- UK GDPR & Data Protection Act 2018;
- Freedom of Information Act 2000;
- Local Government Act 1972;
- Limitation Act 1980;
- HMRC financial retention rules;
- Audit requirements (AGAR);

5.5. Retention Schedule

The Council maintains a Records Retention Schedule that sets out how long each category of data is kept. The following periods apply unless otherwise stated.

5.5.1. Governance

- Minutes (signed): 10 years
- Agendas 6 years
- Reports/background papers:6years

5.5.2. Finance

- Annual accounts: 10 years
- AGAR forms: 6 years
- Bank statements: 6 years
- Invoices, receipts, purchase orders: 6 years
- Budget/precept information: 6 years

5.5.3. Staffing & Councillors

- Personnel files: 6 years after employment ends;
- Payroll records: 6 years;
- Job applications/interview notes: 6 months;
- Register of Interests: held by Basinsgtoke & Deane Borough Council;
- Declarations of Acceptance: Term of office + 1 year.

5.5.4. Property & Assets

- Leases and agreements: 12 years after end;
- Insurance policies: 6 years;
- Inspection logs: 6 years.

5.5.5. Contracts

- Contracts and tenders: 6 years after end

5.5.6. Communications & Community

- Consultation responses: 2 years;
- Mailing lists (e.g., Mailchimp): Until consent withdrawn;
- Correspondence (general): 2 years unless required longer;

5.5.7. Website, IT

- Website backups/logs 90 days;
- Emails: 2 years, unless forming part of an ongoing matter.

5.6. Secure Disposal of Records

Records must be disposed of in a secure and confidential manner.

5.6.1. Paper Records

- Shredding or use of a certified confidential-waste provider

5.7. Digital Records

- Permanent deletion from systems and backups;
- Ensuring processors (e.g., website host, email provider) also delete data.

5.8. Data Retention Exceptions

Information may be kept longer when:

- It is required for legal or regulatory proceedings;
- It is needed for an active complaint, FOI request, or insurance matter;
- Archival value is identified (e.g., historical parish records).

6. Data Breach Policy

6.1. Purpose

The purpose of this policy is to:

- Ensure that personal data breaches are handled promptly and effectively;
- Minimise the risk and impact of any breach;
- Ensure compliance with statutory reporting requirements;
- Provide a clear process for Council Members, and volunteers.

6.2. Definition of a Personal Data Breach

A personal data breach is any incident that results in:

- Unauthorised access to personal data;
- Unauthorised disclosure or sharing;
- Loss or theft of personal data.
- Destruction or alteration of personal data;
- Loss of availability (data cannot be accessed when needed).

Examples include:

- Sending emails to the wrong recipient;
- Loss of an unencrypted laptop;
- Unauthorised access to records;
- Accidental deletion of important files;
- Cyberattacks or system failures.

6.3. Responsibilities

Clerk: Manages breach investigations, maintains records, and liaises with the Information Commissioner's Office (ICO)
Councill Members, and volunteers: must immediately report any suspected data breach.
Council: ensures appropriate safeguards and resources are in place.

6.4. Identifying a Data Breach

Any person working on behalf of the Council must consider whether an incident involves:

- Personal data;
- A breach of confidentiality, integrity, or availability;
- Potential risk or harm to individuals;

If the answer is yes, the incident must be treated as a potential breach.

6.5. Reporting a Breach

All suspected breaches must be reported immediately to the Clerk/RFO, providing:

- Date and time of the incident;
- Description of what happened;
- Type of personal data affected;
- Number and category of individuals involved;
- Any actions already taken.

If the Clerk is unavailable, the Chair or Vice-Chair must be informed.

6.6. Assessment of the Breach

The Clerk will:

- Conduct an initial assessment;
- Determine whether personal data is involved;
- Assess the scale and severity of the breach;
- Identify who is affected and potential consequences;
- Recommend actions to contain and resolve the breach;

Risk factors include identity theft, financial loss, distress, reputational harm, safeguarding concerns.

6.7. Reporting to the ICO

If the breach is likely to result in a risk to individuals' rights and freedoms, the Council must notify the ICO within 72 hours of becoming aware of the breach.
The notification will include:

- The nature of the breach;
- Categories and approximate number of individuals affected;
- Categories and approximate number of data records affected;
- Likely consequences;
- Measures taken or proposed to contain the breach.

If reporting is required, the Council will follow ICO guidance.

6.8. Informing Affected Individuals

Where the breach is likely to result in a high risk to individuals (e.g., identity theft, financial damage, safeguarding issues), the Council will inform individuals as soon as possible, including:

- The nature of the breach;
- What data was affected;
- Actions individuals should take;
- Measures the Council has taken;
- Contact details for further information.

6.9. Managing and Containing the Breach

Actions may include:

- Recovering lost data;
- Changing passwords or access rights;
- Shutting down compromised systems;
- Informing the Council's IT provider;
- Enhancing physical and digital security;
- Reviewing relevant procedures.

6.10. Recording Data Breaches

The Council will maintain a *Data Breach Log*, recording:

- Nature and date of the breach;
- Number of individuals affected;
- Actions taken;
- ICO reporting decision;
- Lessons learned;
- Follow-up actions.

All breaches, regardless of severity, must be logged.

6.11. Learning from Data Breaches

Following any breach, the Council will:

- Review existing policies and procedures;
- Identify areas for improvement;
- Provide additional staff/Councillor training if required;
- Update risk assessments and privacy notices as needed.

7. Privacy Policy

7.1. Introduction

The Council is committed to protecting the privacy and security of personal data. This Privacy Policy explains how the Council collects, uses, stores, and protects personal information in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

7.2. Data Controller

The Council is the Data Controller for the personal data it processes.

Contact:
Clerk
Parish Office
Lady Rose Hall
Laverstoke Lane
Laverstoke
Hants
RG28 7NY
clerk@laverstokeandfreefolk.org.uk
07599 733 607

7.3. What Personal Data the Council Collects

The Council may collect and process the following personal data:

- Contact details: name, address, email, telephone number;
- Correspondence relating to enquiries, complaints, or requests;
- Financial data for payments, grants, salaries, and contracts;
- Employee and Councillor information;
- Consultation responses and public comments;
- Venue hire, or event records (where applicable);
- Supplier and contractor information.

The Council only collects data necessary for its lawful functions.

7.4. How the Council Uses Personal Data

Personal data is used to:

- Respond to enquiries and correspondence;
- Manage services such as hall bookings, community site activities, events, or grants;
- Administer finances, payroll, and payments;
- Publish legally required information (e.g. Councillor details, minutes);
- Consult with the public and fulfil statutory duties;
- Manage contracts, suppliers, and service delivery;
- Comply with legal obligations and audit requirements;
- Provide village e-Newsletter to subscribers.

7.5. Lawful Bases for Processing

The Council processes personal data under the following bases:

- Public task – performing statutory duties and delivering services;
- Legal obligation – compliance with laws, regulations, and audit requirements;
- Contract – where processing is necessary for a contract or service agreement;
- Consent – for eNewsletter when freely given. Otherwise only where required and freely given;
- Vital interests – rare cases concerning health or safety;
- Legitimate interests –mainly for employment or administrative purposes.

7.6. Sharing Personal Data

Personal data may be shared with:

- Contractors and service providers working for the Council;
- External auditors;
- Government bodies (e.g., HMRC);
- Emergency services if required;
- Other authorities where legally required.

Where data is shared, appropriate safeguards are applied.
The Council never sells personal data.

7.7. Retention of Data

Personal data is retained only for as long as necessary and in accordance with recognised local government retention schedules.
When no longer required, data is securely deleted or destroyed.

7.8. How Personal Data Is Stored and Secured

The Council takes appropriate technical and organisational measures to protect personal data.
For details see IT Policy.
Councillors and staff are required to handle data securely.

7.9. Your Rights

Individuals have the following rights under the UK GDPR:

- Right to be informed;
- Right of access;
- Right to rectification;
- Right to erasure (where applicable);
- Right to restrict processing;
- Right to object;
- Right to data portability (rarely applicable to Councils).

Requests should be made to the Clerk. The Council will respond within one month unless an extension is legally permitted.

7.10. Cookies

The Council's website may use cookies to improve user experience.
Users can control or block cookies via their browser settings.

7.11. Data Breaches

The Council will record and investigate all data breaches.
If a breach creates a risk to individuals' rights and freedoms, the Council will notify:

- The Information Commissioner's Office (ICO) within 72 hours;
- Affected individuals where there is a high risk of harm.

A Data Breach Policy and Log are maintained.

7.12. Complaints

If you have concerns about how your data is handled, contact the Clerk in the first instance.
You also have the right to complain to the Information Commissioner's Office:
ICO Website: https://www.ico.org.uk
ICO Helpline: 0303 123 1113

8. Press and Media Policy

All press and media statements must be issued by the Clerk after consultation with the Chair or deputy Chair.

9. Complaints Policy

9.1. Purpose

The council views complaints as an opportunity to learn and improve for the future, as well as a chance to put things right for the person that has made the complaint.

9.2. Complaints

The complaints handling policy is:

- A complaint may come from any person or organisation who has a legitimate interest in the council. A complaint can be received verbally, by phone, by email or in writing.
- A complaint is any expression of dissatisfaction, whether justified or not, about any aspect of the Council;
- The Clerk will be a point of contact for all complaints (unless the compliant concerns the actions of the Clerk);
- Any complaint received will be promptly communicated to all Councillors;
- The Council will promptly review and investigate any complaint in a fair and timely way;
- The Council will respond the complaint, wherever possible, in a way that the complaint is resolved and that relationships are repaired;
- All complaint information will be handled sensitively, telling only those who need to know and following any relevant data protection requirements.

10. Donations Policy

10.1. Purpose

This policy sets out how the Council will:

- accept and record donations and fundraising income;
- run a special appeal to support the purchase of a community asset.

10.2. Accepting Donations

The Council may accept donations that:

- support the Council's purposes and provide community benefit; and
- do not create conflicts of interest or improper influence.

The Council will refuse or return donations that:

- are conditional on the Council acting unlawfully or improperly; or
- create unacceptable reputational risk; or
- are offered to influence planning, licensing, or procurement decisions.

10.3. How donations are received and recorded

Donations may be accepted via bank transfer or an approved fundraising platform.
The Clerk will ensure:

- prompt banking;
- a clear audit trail (date, amount, payer where known, method, purpose);
- correct ledger coding (unrestricted vs earmarked); and
- regular reporting through budget monitoring.

10.4. Acknowledgements and publicity

Donors may be thanked publicly unless they request anonymity.
Donor recognition must not imply preferential treatment or procurement advantage.

10.5. Earmarked funds

The Council may establish an earmarked fund to hold donations and fundraising income intended to support a specific project and directly related costs.
Cash held in earmarked funds will only be used for purposes stated in the appeal related to the fund.

10.6. Appeals

The wording of any appeal must be clear.
All appeal materials must state:

- the purpose (what the money is for);
- whether donations are refundable if the project does not complete
- how any costs are paid for if the project does not complete; and
- what will happen to any surplus

The Council will also manage any conflicts of interest (declarations and non-participation where required).

10.7. Donor Contact details

Contact details will be collected to meet Governance requirements.

11. Employment Policy

11.1. Introduction

This Employment Policy sets out the principles and procedures by which the Council manages its employees. It ensures compliance with UK employment legislation and promotes fairness, transparency, and accountability in all employment matters.

11.2. Recruitment and Appointment

- All recruitment will be conducted fairly and openly;
- Vacancies will be advertised appropriately to ensure equal access;
- Job descriptions and person specifications will be prepared for each role;
- Successful candidates will receive a written contract of employment.

11.3. Terms and Conditions of Employment

- Employees will be appointed under written contracts in line with statutory requirements;
- Hours of work will be specified in contracts, with flexibility considered where appropriate;
- A probationary period of up to six months may apply to new employees;

11.4. Equal Opportunities

- The Council is committed to equality of opportunity in employment;
- No employee or applicant will be discriminated against on the grounds of age; disability, gender, race, religion, sexual orientation, or marital status;
- Reasonable adjustments will be made to support employees with disabilities.

11.5. Employee Conduct

- Employees are expected to act with integrity and professionalism at all times;
- Confidentiality of Council business must be maintained;
- Respectful behaviour towards Councillors, colleagues, and members of the public is required.

11.6. Leave and Absence

- Employees are entitled to statutory annual leave, plus public holidays, as set out in their contract;
- Sick leave must be reported promptly to the Chair or other designated Councillor;
- Family leave (maternity, paternity, adoption, parental) will be granted in accordance with statutory provisions.

11.7. Training and Development

- The Council will support employees in undertaking relevant training;
- Employees are encouraged to pursue continuous professional development;

11.8. Grievance Procedure

- Employees may raise concerns through a formal grievance procedure;
- Grievances should be submitted in writing to the Chair;
- The Council will deal with grievances promptly, fairly, and in line with the ACAS Code of Practice.

11.9. Disciplinary Procedure

- The Council may take disciplinary action where conduct or performance falls below expected standards;
- Procedures will include verbal warnings, written warnings, and dismissal if necessary;
- Employees have the right to appeal against disciplinary decisions.

11.10. Health and Safety

- The Council is committed to providing a safe working environment;
- Risk assessments will be carried out for all relevant tasks;
- Employees must comply with health and safety requirements and report hazards promptly.

12. Safeguarding Children and Vulnerable Adults Policy

12.1. Purpose and Objectives

The purpose of this policy is to guide Council Members and volunteers should any child protection issue or any issues with vulnerable adults arise during any activity associated with the Council.

The Council does not directly provide care of supervision services to children and vulnerable adults. The Council's Community Site is used by other organisations under both long-term leases and short-term licences for services to children and vulnerable adults.

The objectives of this policy are:

- To ensure that where possible all activities offered by the Council are designed and maintained to limit risk to children and vulnerable adults;
- To promote the general welfare, health and development of children by being aware of child protection issues and to be able to respond where appropriate as a local government organisation and as a landlord to other organisations;
- To develop procedures in recording and responding to accidents and complaints and to alleged or suspected incidents of abuse and neglect.

12.2. Safeguarding Officer

The Clerk will act as Safeguarding Officer and will act as the main point of contact for all safeguarding issues and is responsible for ensuring compliance with this policy.

12.3. Direct Activity: Responsibilities & Procedures

The Council will ensure that:

- before any Council organised event with children or vulnerable persons, that a risk assessment is carried out and participants are briefed appropriately;
- whilst Council Members are unlikely to be involved with children during the performance of their duties, they are aware and mindful of the risks that may arise;
- the Clerk is DBS checked in order to enter the day nursery in Lady Rose Hall during nursery hours and then only with the permission of and in the presence of nursery staff;
- the Clerk's DBS check is renewed at least every 3 years;
- before any volunteers or staff are recruited to work with children and vulnerable persons, they are interviewed, two satisfactory references are taken up and required DBS checks are carried;
- Council Members will adhere to the 'List of Recommended Behaviour' namely:
    - A minimum of two adults present when supervising children.
    - Not to play physical contact games.
    - Adults to wear appropriate clothing at all times.
    - Ensure that accidents are recorded in an accident book.
    - Never do anything of a personal nature for a young person.
- any safeguarding allegations or incidents made to any Council Member are reported to the Safeguarding Officer. Any such allegation will be recorded in an Incident book. The incident book will be available at every Council meeting for inspection by Councillors. The Safeguarding Officer is responsible for ensuring the matter is handled in accordance with the Local Safeguarding Children Board procedures and also referred to the Council for further action as appropriate and future risk assessment.

12.4. Facilities – Responsibilities & Procedures

The Council's Community Site is used by other organisations under both long-term leases and short-term licences for services to children and vulnerable adults. The Council does not have any direct oversight of these activities.

The Council will ensure that:

- new leases and licences are only given to reputable organisations that have their own appropriate Safeguarding Policies and that the Leases and Licence conditions address any safeguarding matter that may impact the Council;
- the terms of hire of the village hall require that all children and vulnerable adults using the hall to do so with the consent and the necessary supervision of a parent, carer or other responsible adult;
- information received about protection for children and vulnerable adults and good practice is shared with partner organisations when appropriate;
- work by contractors employed by the Council on facilities is arranged for times when the facilities are not in use by children or vulnerable adults. If this is impractical the contractor will be asked to provide their Safeguarding Policy which will be reviewed to ensure that necessary safeguards are in place.
- if any safeguarding concerns are raised about an organisation using the Council's facilities the concerns are reported to the Safeguarding Officer who will seek advice on the appropriate action to take.

12.5. Declaration

The Council is fully committed to safeguarding the well-being of children and vulnerable adults by protecting them from physical, sexual, emotional harm and neglect.
All Council Members should read the Safeguarding Policy. Having read the Policy, they should be proactive in providing a safe environment for children and vulnerable people who are involved in Council activities.
Useful safeguarding information:
https://www.basingstoke.gov.uk/safeguarding
https://www.hants.gov.uk/socialcareandhealth/childrenandfamilies/safeguardingchildren/childprotection/mash

13. RISK MANAGEMENT POLICY

13.1. Introduction

The Council is committed to ensuring that risks are properly identified, evaluated, and managed so that it can deliver services effectively, safeguard public funds, and comply with legal and statutory obligations. This policy sets out the Council's approach to risk management in accordance with proper practices.

13.2. Definition of Risk

A risk is any event or situation that may adversely affect the Council's ability to achieve its objectives. The Council recognises the following categories of risk:
Financial– fraud, error, budget overspend, loss of income;
Operational– failed processes, contractor issues, asset failure;
Legal/Regulatory– non-compliance with legislation or governance requirements;
Health & Safety– accidents, unsafe working environments, lack of assessments;
Reputational– loss of public confidence, complaints, data breaches;
Strategic– long-term planning, major projects, staffing capacity.

13.3. Roles and Responsibilities

The Council: has overall responsibility for effective risk management, approves the policy, and reviews the Risk Register at least annually.
The Clerk: responsible for day-to-day management of risk, maintaining the Risk Register, reporting new or emerging risks, recommending controls, and ensuring compliance with policies and regulations.
Committees/Working Groups: Assist in monitoring risk in their areas, identifying and reporting concerns, and overseeing specific high-risk projects.
Internal Auditor: Provides independent assurance on financial and governance controls.
Chair/Vice-Chair: Provide oversight and ensure risk is considered during decision-making.

13.4. Risk Identification

Risks may be identified through:

- Annual review of the Risk Register;
- Budget preparation and monitoring;
- Internal and external audit reports;
- Inspections of assets and facilities;
- Insurance renewals and claims;
- Reports from the Clerk, Councillors, contractors, or members of the public;
- Changes in legislation, staffing, or service delivery.

13.5. Risk Assessment Method

The Council assesses risks using two measurements:

- Likelihood – the probability of the risk occurring
- Impact – the severity of the consequences

Risks are scored on a Low/Medium/High basis or numerically (e.g., 1–5). Higher-scoring risks require enhanced controls to mitigate risk.
Risks are reevaluated when enhanced controls are in place.

13.6. Risk Register

The Council will maintain a Risk Register listing each identified risk, its category, likelihood, impact, controls in place, required actions, and impact of control mitigation.

13.7. Risk Monitoring and Review

The risk monitoring and reviews are:

- An annual review of the Risk Register by Council will occur annually, usually alongside the review of policies or the budget-setting process;
- Amendments may be made at any time when risks change or new risks emerge, or after any major incident, change in legislation, or identification of a new risk.

14. Investment Policy

The Council's investment policy is that:

- all reserves shall be held as cash deposits held with regulated institutions;
- deposits with any one institution shall not exceed the FCCS deposit protection limit;
- at least £20,000 shall be maintained in no- notice deposit accounts;
- no term deposits shall exceed one year and the maturity of tranches of deposits shall be spread during the year or allocated to different maturities.
- the set-up of term deposits must be approved by the Council.

15. Reserves Policy

15.1. Introduction

Reserves are held to ensure that the Council can meet unexpected costs and future financial obligations and to also enable the Council to spread the cost of non-regular costs between years without changes to the precept. The Community Site is a major asset managed by the Council and it has significant financial obligations for the maintenance of the site. Reserves are held to ensure these obligations can be met.

The Council also has an obligation to Council rates payers not to hold excessive reserves while charging a precept.

15.2. General and Earmarked Reserves

General Reserves are funds that do not have restrictions on their use and are used spread the impact of uneven cash flows and to cover unexpected events.
Earmarked Reserves are funds held for specific purposes or projects. They are available to deliver a defined project, cover known expenditure or future liabilities arising from assets or contracts.

15.3. Reserves Policy

The target reserves policy is to hold:

- A General Reserve of between 40% to 100% of precept to meet non-regular and unexpected costs.
- Earmarked Reserves for:
  - 100% of any hirer deposits;
  - 100% of any committed expenditure in excess of £500;
  - A reserve of up to 100% of the expected costs net of grants of any Projects approved by the Council;
  - Community Site costs and obligations. The reserve shall be held as a fund for any costs relating to the Community Site contracts. The reserve shall be at least 50% of the budgeted annual income of the Community Site. The targeted reserve shall be the greater of a) the 100% of the projected shortfall in income over expenditure during the next 5 years, and b) the expected financial liability for the Community Site as determined by a Community Site financial model. The model shall be prepared on a prudent basis.

15.4. Council Approval of Reserves

The Council will review reserves as part of the budget approval.
The Council must approve:

- the set up any new earmarked reserves for a Project; and
- The release or transfer of an earmarked reserve for a purpose other than the specific purpose for which it is held.

16. Grants Policy

16.1. Introduction

The Council will consider requests for grants from outside organisations. The power of the Council to award grants is limited and must be in accordance with Local Government Act s137 and Local Government (miscellaneous provisions) Act 1976 s 19.

16.2. Grants Policy

The grants policy is:

- all grants must be approved by Council;
- grant requests can be received from:
  - Clubs and societies within Laverstoke and Freefolk Parish;
  - Clubs and Societies outside Laverstoke and Freefolk parish but serving the people of Laverstoke and Freefolk.
- grant requests must:
  - provide full information about the project and use of the grant;
  - the amount of grant requested;
  - be accompanied by the Council's application form, the latest set of accounts and a latest bank statement from the organisation making the request.
- grants cannot be made retrospectively.
- proof of expenditure will be required on completion of the project.
- the Council has the right to refuse a grant application without explanation.

16.3. Application form

The grant application form is available from the Clerk.