# Bersted Parish Council
# Information Security Policy

**Bersted Parish Council**

**2018**

## Document Control

| | |
|---|---|
| **Organisation** | Bersted Parish Council |
| **Title** | Information Security Policy |
| **Creator** | Cllr Trevor Marshall MSc |
| **Distribution** | Public |
| **Filename** | |
| **Owner** | Bersted Parish Council |
| **Subject** | Security of Information and Information Systems used by Bersted Parish Council |
| **Date Adopted** | 13-02-2018 |
| **Review date** | February 2019 |

## Document Amendment History

| Revision No. | Originator of change | Date of change | Change Description |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Summary**
This document is intended to prevent unauthorised disclosure of information by laying down clear standards of practice to maintain good security when handling sensitive or confidential information within Bersted Parish Council
.

**Contents**

# Information Security Policy

## 1. Introduction

The objective of the Bersted PC Information Security Policy (ISP) is to ensure that sensitive and confidential information used to deliver our services is treated with appropriate security by all who handle it. 'Appropriate' is a degree of precaution and security proportionate to the potential risk and impact of loss or accidental disclosure.

It is not possible to set out precautions and actions to cope with all circumstances and conditions, therefore anyone handling sensitive and confidential information MUST take personal responsibility and make considered judgements in terms of how they handle this information whilst delivering their service. If in any doubt they should seek clarification from the Parish Clerk or the Councillor with responsibility for oversight of this Policy.

Overall impact is determined by the degree of sensitivity of the information and the quantity involved, but you must remember that a single record about an individual can have a potentially significant impact on that individual if accidentally disclosed to others.

## 2. Policy statement

It is the policy of Bersted Parish Council (the Council) that we will protect information from a loss of:

- confidentiality (ensuring that information is accessible only to authorised individuals)
- integrity (safeguarding the accuracy and completeness of information)
- availability (ensuring that authorised users have access to relevant information when required)
- relevance (only keeping what we need for as long as it is needed)

We will meet all regulatory and legislative information management requirements.
We will maintain business continuity plans.
We will deliver appropriate information security training to all staff.
We will make available appropriate and secure tools to all staff.
We will report and follow-up all breaches of information security, actual or suspected.

## 3. Scope and application

The Bersted PC Information Security Policy covers the creation, acquisition, retention, transit, use, and disposal of all forms of information.

The Policy applies to:

- **Everyone**. The policy applies to all information held by the council which includes information held on its behalf by partners/contractors and all council Members, permanent, contract and temporary employees, and all third party people who have access to Bersted PC premises, systems or information. We refer to all these as "Everyone" in this policy.
- **All council information**. The policy applies to all systems, software and information created, held, processed or used on those systems or related media, electronic, magnetic, or written/ printed output from Bersted PC systems. It also applies to all means of communicating information, both within the council and externally.

Some examples of information that is covered by this policy:

- data and voice transmissions or recordings,
- post,
- email,
- sms/text,
- cameras,
- whiteboards,
- memory sticks,
- discs,
- fax
- image/sound processing,
- video-conferencing,
- photocopying,
- flip charts,
- general conversation etc.

## 4. The legal basis

The Council must comply with all relevant UK and European Union legislation, including:

• Human Rights Act 1998
• Data Protection Act 1998 and 2018
• Freedom of Information Act 2000
• Common law duty of confidence
• Copyright, Designs and Patents Act 1988
• Computer Misuse Act 1990
• Regulation of Investigatory Powers Act 2000
• Health & Social Care Act 2001
• Health and Safety at Work Act 1974

The requirement to comply with this legislation extends to everyone as set out at 3.2 above who are held personally accountable for any breaches of information security for which the Council is responsible.

## 5. Definitions

### Information and data

Information results from the acquisition and collation of data and expressed views and opinions based upon it. It can be held and used in many forms including, but not limited to, electronic records, hard copy (paper, fiche) phone calls and conversations. For the purpose of this policy information and data can be regarded as the being the same.

### Sensitive and confidential information

The following list is not exhaustive and contains examples of sensitive and confidential information:

- Person-identifiable information, e.g. service user and employee records
- Council business or corporate records containing organisationally or publicly sensitive information

- Any commercially sensitive information such as information relating to commercial proposals or current negotiations
- Politically sensitive information
- Information relating to security, investigations and proceedings
- Information provided in confidence

An easy sense check on whether information is sensitive or confidential is:

- Is the information covered by the Data Protection Act 1998 or any further duty of confidence?
- Could release of the information cause problems or damage to individuals, the public, the Council or a partner organisation? This could be personal, financial, reputation or legal damage.
- Could release of the information prejudice the outcome of negotiations or investigations?

If in doubt seek advice from the Parish Clerk and err on the side of caution, treating the information as sensitive and confidential.

**6. Governance and accountabilities**

The **Senior Information Risk Owner** (SIRO) is the Parish Clerk and is the focus for the management of information security. The Full Council will be requested to approve resources required to support the ISP and procedures. The SIRO will ensure that the ISP and resources are integrated into Council processes appropriately and within the business context.

**Full Council** is responsible for ensuring that all employees, contractors and partner organisations with legitimate access to information held on the Council's behalf within their department are familiar and compliant with their responsibilities under the Data Protection Act 1998, the Freedom of Information Act 2000 and other relevant legislation as well as the relevant policies and standards of the Council.

**Full Council** will approve policies and strategic plans in support of the ISP and work together across departments, with external agencies and service delivery partners, to ensure that compliance with the ISP is maintained.

**The Parish Clerk** is responsible for co-ordinating all Data Protection and Freedom of Information activities within the Council, helping and advising departments, monitoring compliance with the Acts and acting as the point of contact with the Information Commissioner's Office.

**7. Management of Information**

The Council will manage information in accordance with the principles and procedures within this policy and annex.

It is important that the public and our partners have confidence in our ability to handle sensitive and confidential information appropriately. The following principles apply:

- All identifiable personal information is to be treated as confidential and will be handled in accordance with the relevant legal and regulatory protocols.
- All identifiable information relating to staff is confidential except where national policy on accountability and openness requires otherwise.

- All departments will maintain procedures to ensure compliance with the Data Protection Act 1998, The Human Rights Act 1998, the common law duty of confidentiality, the Freedom of Information Act 2000 and any other relevant legislation or statutory obligation.
- Information must be recorded, used and stored to protect integrity so that it remains accurate and relevant at all times.

**7a. Passwords**
Passwords will be created using a minimum of 8 alphanumeric characters and upper and lower case. They will be kept confidential to the user at all times and only given when requested by the Parish Clerk for the purposes of Audit. Passwords will be changed as requested.

**8. Creation of records**
The Council will create and maintain adequate records to meet the Council's business needs and to account fully and transparently for all actions and decisions. Such records should provide credible and authoritative evidence; protect legal and other rights of the Council, its staff and those who have dealings with the Council; facilitate audit; and fulfil the Council's legal and statutory obligations.

**9. Access to Records**
Information will be made available on request to anyone who has a right to see it under relevant legislation such as the Data Protection Act 1998 or the Freedom of Information Act 2000.

**10. Openness and Transparency**
Information will be made accessible:

- to anyone, in ways that suit their needs and engenders public trust and confidence in the Council's operations and in compliance with Data Protection and Freedom of Information legislation
- to Council staff where it is necessary for the delivery of their services and the discharge of their duties
- to our partners, where it is necessary for the delivery of joint services and in the interests of our community and in accordance with agreed information sharing protocols.

**11. Information Sharing**
Sensitive and confidential information will be shared with other organisations only where there is a need or obligation to do so. Where there is a need to enable service delivery the information sharing will be governed either under the terms of a contract or information sharing agreement. The Council will also share information as required by law.
You must not use standard USB data sticks, CDs or other removable media as portable temporary storage for electronic files and documents unless they have been encrypted. Use of any other USB devices not supplied by Bersted Parish Council is prohibited.

**12. Records Management**
Records will be managed and controlled effectively to fulfil legal, operational and information needs and obligations in the most cost-effective manner.

**13. Data Quality and Assurance**
The Council will ensure that information is accurate at the time of capture and will be subsequently maintained to ensure accuracy, integrity and consistency across systems and datasets as set out in the Council's Data Quality Policy and Strategy.

**14. Handling sensitive or confidential information**
Information and the underlying data have a lifecycle covering creation/acquisition, maintenance and use, disclosure, storage and disposal. Annex A sets out the *minimum* standards for handling sensitive and confidential information. Failure to adhere to these standards may result in disciplinary or other appropriate action.

**15. Information Systems Acquisition, Development and Maintenance**
The Parish Clerk will ensure that all new information systems, applications and networks include a risk assessment and remedial actions as necessary.
System owners will develop and maintain System Operating Procedures for systems under their control to ensure compliance with this policy.

**16. Technical Compliance**
The Parish Clerk is to ensure that information systems are checked regularly for technical compliance with relevant security implementation standards. Operational systems will be subject to technical examination to ensure that hardware and software controls have been correctly implemented.

**17. Business Continuity**
The Council's business continuity planning process will include consideration of information security gained from the information asset and risk register.

**18. Risk Management**
Risk management will be conducted to register information assets, assess the risks to those assets, evaluate the impact of those risks and control, modify or mitigate against the risks. Overall responsibility will rest with the SIRO who will direct risk management.
The plan will be implemented by:

- Maintaining a corporate asset register
- Conducting risk assessment
- Applying risk mitigation in context with business demands
- Measuring results and improving the process from lessons learned
- Implementing training and awareness programmes
- Implementing procedures for the detection and control of security events and incidents

**19. Quality Assurance and Audit**
The Information Security policy, standards and procedures will be audited periodically as part of the annual Internal Audit work plan.

**20. Culture and Awareness**
This policy is supported by a positive information security culture programme running through the Council. The Parish Clerk and Deputy Clerk will consider and recommend initiatives to Full Council to promote and maintain positive awareness.

**21. External Assurance**
We will promote to all of our residents, customers, third parties and partners our commitment to information security. The Council will provide this assurance on a regular basis.

**22. Employees**
Pre-employment checks on candidates we are going to appoint for employment and contracts will be carried out in accordance with relevant laws and regulations and proportional to access to information and business requirements.
Information Security will be included in job descriptions and person specifications as appropriate. Personal objectives and training for employees will be agreed as part of the appraisal process and will include the practice and encouragement of Information Security.
All new employees and Councillors will undergo induction in Information Security, Data Protection and Freedom of Information, covering the principles and legal aspects. Subsequently, all employees will undertake further or refresher training as required to maintain safe access to sensitive and confidential information.

**23. Partners and Third Parties**
The Parish Clerk will ensure that contractors, partners and third parties agree to terms and conditions consistent with the Council's ISP. Access to and handling of Council information will be managed through procurement and partnership arrangements and subject to appropriate agreements and monitoring, including site visits where necessary and practicable.
Council Officers will also report any known security breaches by partners and third parties, even if the breach does not involve the Council, in order to monitor their general security standards.

**24. Handling Information Security Incidents**
Any loss of sensitive and confidential information, either actual or suspected, must be reported immediately to the Parish Clerk or the Deputy Parish Clerk if they are not available.
The incident will be handled in the first instance by Parish Clerk who will notify other parties as required.

**25. Breaches of policy**
Where Council members, employees or service delivery partners have acted in accordance with this standard, but a breach occurs through the action of others, they will be deemed to have acted reasonably.
However, if Council members, employees or service delivery partners are found to be in breach of the policy and its guidance then they may be subject to disciplinary or other appropriate action.

**Information Security Policy - Annex A**
**Standards for handling sensitive or confidential information**
The following standards are set out for all members, employees and service delivery partners as the *minimum* standards for handling sensitive and confidential information. Failure to adhere to these standards may result in disciplinary or other appropriate action.

## A.1 Creation/acquisition
When information is acquired and records created there are some simple principles you must follow:
You must ensure that it is:

- accurate (factual or qualified expert opinion)
- up to date (changes updated as soon as possible)
- consistent (the same information across different datasets)
- relevant (only as much and for as long as needed for the intended purpose)

When acquiring and handling personal information you must comply with the processes and standards set out under the Data Protection Act 1998.

## A.2 Maintenance and use
Information and records must be maintained to ensure that they are accurate, up to date and consistent. When using sensitive or confidential information there are some ground rules you must follow to maintain confidentiality and integrity:

- never leave the information where others could see it e.g. on a desk, computer screen or left on a fax or printer
- do not discuss the information where others not authorised may overhear
- only use the information for the purpose for which it was collected
- changes must be recorded as soon as possible after the change occurs
- always store information securely, following filing procedures in structured file systems
- always put the information/records back as soon as you have finished using them
- do not produce copies unless they are needed and always update the master record, securely destroying copies as soon as they are no longer needed
- review the information regularly to ensure it is accurate and up-to-date
- if information and records are taken from a secure location the risk of loss increases and you must follow the standards set out in the Data in Transit policy

## A.3 Disclosure
Prior to disclosure of sensitive and confidential information you should be satisfied that at least one of the following applies:

- for personal data, one of the conditions for processing set out in Schedule 2 to the Data Protection Act 1998 are satisfied

- for sensitive personal data, one of the conditions for processing set out in Schedule 2 and one of the conditions for processing set out in Schedule 3 of the Data Protection Act 1998 are satisfied
- disclosure is permitted under one of the exemptions set out in the Data Protection Act 1998; (e.g. the prevention or detection of crime, the capture or prosecution of offenders, and the assessment or collection of tax or duty)
- disclosure is in the public interest, (e.g. for safeguarding national security or for preventing harm to children or adults)
- a relevant information sharing agreement is in place
- there is a legal or statutory obligation to disclose the information
- disclosure is governed by and in accordance with contractual terms and conditions

You must never disclose sensitive and confidential information to anyone who does not have a right to see it.
If you are unsure do not disclose the information. Seek advice from the Parish Clerk.

**A.4 Storage**
All sensitive and confidential information must be stored securely and access allowed only to those who need it for legitimate purposes.
Standards for handling sensitive and confidential information:

- Secure storage can be secure buildings with access controls to the building, specific floors and individual offices. The controls can be swipe cards, keypads, key locks etc. Appropriate measures must be used depending on the sensitivity of the information and who should have access to it.
- Similarly access to electronic information must be controlled by the use of passwords and assigned permissions within the systems that hold the information.
- To ensure appropriate access under these controls you MUST NOT let others use your access whether it is a swipe card, key, login or system password or other access control.

**A.5 Disposal**
When disposing of any sensitive and confidential information you must comply with the Council's Retention and Disposal Schedules for the specific information and records being disposed.
When disposing of hard copy sensitive and confidential information you must always use secure methods such as cross-cut shredding or pulping or the confidential waste bins where available and keep the waste in a secure place until it can be collected for secure disposal. NEVER put sensitive and confidential waste in normal waste bins. Electronic storage on any office equipment disposed of must securely wiped and be physically destroyed.