

Doddinghurst Parish Council Data & Information Security Policy

Issue date:	February 2010	Review date:	February 2011
Version Issue:	1.1	Issued by:	Roger Blake

Aim:	To establish the Information and Data Policy for Doddinghurst Parish Council
-------------	--

Scope:	To meet the needs of the Council & ICO Data Commissioner
---------------	--

Associated documentation:	Legal Framework: The Data Protection Act (1998), Copyright Designs & Patents Act (1988), Computer Misuse Act (1990), Health & Safety at Work Act (1974), Information Commissioners Office Data Commissioner registration. Policies: Staff employment terms and conditions
Appendices:	None
Approved by:	By resolution of the Full Council
Date:	4 th March 2010

Review and consultation process:	To become part of the annual governance review of the Council carried out by the Finance and resource Committee
Responsibility for Implementation & Training:	The Clerk and RFO for the Council

HISTORY

Revisions:		
Date:	Author:	Description:
11/02/2010	R Blake	Initial Issue
16/02/1010	R Blake	Amended to V 1.1

Distribution methods:	By email to councillors and both paper and electronic copies retained on file.
------------------------------	--

1. Introduction

This top-level information security policy is for publication and is a key component of Doddinghurst Parish Councils overall information security management documentation. The Council also maintains a Data and Information Security Review and Risk Assessment document that is confidential to the Council.

Doddinghurst Parish Council Data & Information Security Policy

Doddinghurst Parish Council is a small/ medium sized T1local Council. The documentation it keeps and holds is mainly already in the public domain and no information of national, regional or area security nature whatsoever is kept. Information and Data is only confidential where it relates to commercially sensitive material provided by potential contractors for work to be done and personal information relating to its employees.

2. Objectives, Aim and Scope

2.1. Objectives

The objectives of Doddinghurst Parish Council Information Security Policy are to preserve:

- **Confidentiality** - Access to Data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All related assets and networks shall operate correctly.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

2.2. Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by Doddinghurst Parish Council by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principals of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

2.3. Scope

This policy applies to all information, information systems, networks, applications, locations and users of Doddinghurst Parish Council or supplied under contract to it.

3. Responsibilities for Information Security

3.1. Ultimate responsibility for information security rests with the Body Corporate of Doddinghurst Parish Council, but on a day-to-day basis the Clerk or Deputy Clerk shall be responsible for managing and implementing the policy and related procedures.

3.2. Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of:-

- The information security policies applicable in their work areas

- Their personal responsibilities for information security
 - How to access advice on information security matters
- 3.3.** All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.
- 3.4.** The Information Security Policy shall be maintained, reviewed and updated by the Finance and Resource Committee annually.
- 3.5.** Line managers shall be individually responsible for the security of their physical environments where information is processed or stored.
- 3.6.** Each member of staff shall be responsible for the operational security of the information systems they use.
- 3.7.** Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.
- 3.8.** Contracts with external contractors that allow access to the organisation's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

4. Legislation

- 4.1.** Doddinghurst Parish Council is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the Doddinghurst Parish Council, who may be held personally accountable for any breaches of information security for which they may be held responsible. Doddinghurst Parish Council shall comply with the following legislation and other legislation as appropriate:

- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Health & Social Care Act 2001

5. Policy Framework

5.1. Management of Security

- Responsibility for Information Security shall reside with the Body Corporate of Doddinghurst Parish Council.
- Doddinghurst Parish Council's Clerk (or Deputy Clerk when acting as the Clerk) shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organisation.

5.2. Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.

- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

5.3. Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.
- Information security expectations of staff shall be included within appropriate job definitions.

5.4. Security Control of Assets

The IT asset's, (hardware and software application) is in the custody of the Clerk (or the Deputy Clerk when acting as the Clerk) who shall be responsible for the information security of that asset. Individual elements of Data may be in the custody of the Clerk or the Deputy Clerk who shall be responsible for the information security of that individual element of data.

5.5. Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

5.6. User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

5.7. Computer Access Control

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

5.8. Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

5.9. Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

5.10. Computer and Network Procedures

Management of computers and networks, including websites, shall be controlled through standard documented procedures that have been authorised by the Doddinghurst Parish Council Finance and Resource Committee.

5.11. Information Risk Assessment

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature

of Doddinghurst Parish Council's risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

5.12. Information security events and weaknesses

All information security events and suspected weaknesses are to be reported to the Clerk without delay. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

5.13. Classification of Sensitive Information.

Doddinghurst Parish Council shall implement appropriate information classifications controls as follows:

The classification **PC Confidential** - shall be used to mark all sensitive information such as contractual and employee records. It shall cover information that the disclosure of which is likely to:

- adversely affect the reputation of the organisation or its officers or cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness of the organisation;
- cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- breach statutory restrictions on disclosure of information;
- disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

PC Confidential documents should be stored in lockable cabinets

5.14. Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy.

5.15. Monitoring System Access and Use

The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime

Doddinghurst Parish Council Data & Information Security Policy

- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act

5.16. Accreditation of Information Systems

The organisation shall ensure that all new information systems, applications and networks include a security plan and are approved by the Clerk before they commence operation.

5.17. System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Clerk.

5.18. Intellectual Property Rights

The organisation shall ensure that all information products are properly licensed and approved. .

5.19. Business Continuity and Disaster Recovery Plans

The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

5.20. Reporting

The Clerk shall keep the Finance and resource Committee informed of the information security status of the organisation by means of regular reports and presentations.

5.21. Policy Audit

This policy shall be subject to audit by the Internal Auditor, the External Auditor and Information Commissioners Office.

5.22. Further Information

Further information and advice on this policy can be obtained from The Clerk, at clerk@doddinghurst-pc.gov.uk.

6. Policy approved by the Chairman to the Council Deborah Dicker:

Signature

Date: 4th March 2010