



Great Yarmouth Borough Council IT Security Policy

Author	Geoff Jones
Date	17 March 2009
Version	2.1
Last Review Date	2 March 2011
Review Changes	General advice added for DPA exemptions
Document Status	Final

1.0 INTRODUCTION	3
1.1 POLICY RATIONALE	3
1.2 SCOPE	4
1.3 PRINCIPLES	4
2.0 IT SECURITY POLICY	5
2.1 GENERAL POLICY	5
2.2 POLICY STATEMENT	5
2.3 IT EQUIPMENT	5
2.4 IT SYSTEMS AND DATA	6
2.5 PASSWORD SECURITY	6
2.6 SECURED AREAS	7
2.7 GENERAL	7
3.0 IMPLEMENTATION AND COMPLIANCE	7
3.1 IMPLEMENTATION	7
3.2 COMPLIANCE	8
4.0 EQUALITY IMPACT ASSESSMENT	8
5.0 HEALTH AND SAFETY	8
6.0 REFERENCE DOCUMENTS	9
7.0 DISTRIBUTION	9
8.0 REVIEW	9
APPENDIX A	10
APPENDIX B	12

1.0 INTRODUCTION

This policy forms part of the suite of policies dealing with data security.

The use of developing technology within Great Yarmouth Borough Council is an essential business requirement to keep in step with the demands for the retrieving, collating and communication of information, in a fast, economic and secure manner.

The aim of this IT Security Policy is to reduce the risk to the integrity of the resources and reputation of Great Yarmouth Borough Council, while maximising the use of IT based technology as an important business tool.

1.1 POLICY RATIONALE

At the time of the writing of this IT Security policy in 2009, the council was aiming to meet the requirements to obtain and use a government connect secure circuit.

In 2009, the Council was of the view that there was a need to ensure that an agreed standardised approach was being taken to IT Security, in order to protect Council assets, and to ensure compliance with audit requirements.

This policy seeks to establish a standard set of conditions, and a framework for IT Security within the Council.

Service managers are responsible for ensuring that all employees and agents are trained in using the IT resources and that they have read and signed this document, so that users are aware of the requirements of the IT security policy.

The policies set out in this document are intended to address IT security concerns and to protect the name and reputation of Great Yarmouth Borough Council.

The computer systems of Great Yarmouth Borough Council and the confidential information contained upon them are an **essential resource** and require **adequate protection**.

Failure by **any user** to adhere to these policies or any other misuse of the IT resources may result in **disciplinary action**.

Misuse of Great Yarmouth Borough Council IT resources could have serious consequences including, but not limited to dismissal, criminal prosecution or civil liability.

1.2 SCOPE

This Policy will apply to all Council employees.

1.3 PRINCIPLES

The Policy is designed to ensure that there are clear internal arrangements for the effective management of IT Security.

2.0 IT SECURITY POLICY

2.1 GENERAL POLICY

For the purposes of this policy the following definitions apply-

IT - Electronic processing, storage, transmission and display facilities involved in such equipment as computers, word processors and compatible apparatus.

Personal data - Data which refers to any living individual.

2.2 POLICY STATEMENT

In view of the Council's heavy reliance on data processing systems, and in line with the obligations prescribed by GovConnect the confidentiality, security and accurate processing of data are of paramount importance. If there are delays or curtailment in data processing, serious inconvenience and even financial loss may occur.

To help maintain equipment, systems and data in a sensibly controlled environment there are a number of requirements to be observed which are set down in this document.

This document reflects the Council's response to the Data Protection (see Appendix A). The Freedom of information Act, the council's policy on data quality and its adherence to the requirements of GovConnect.

You should be aware of the implications of the Computer Misuse Act (see Appendix B).

Any breach of this policy may result in disciplinary action, under the existing terms of the Council's Conditions of Service.

You should also be aware of any EC regulations regarding information technology which may be issued from time to time. You will be informed of any relevant regulations when they are produced.

2.3 IT EQUIPMENT

Heads of Departments are responsible for IT equipment under their control and for its proper use.

The use of equipment for purposes not directly concerned with the Council's business is not allowed.

Only persons authorised by the Head of Department (or his designated officer)

may operate IT equipment.

IT equipment must have security facilities appropriate to the sensitivity of the data held. The axiom is "if in doubt, protect it"-

2.4 IT SYSTEMS AND DATA

All computer systems and data developed or purchased for the Council are for the sole use of the Council.

Deliberate unauthorised access to, copying, alteration, or interference with computer programs or data is not allowed.

The use of unlicensed software is illegal and is not allowed.

A serious view will be taken of any unauthorised disclosure of information from computer input or output, this could result in disciplinary action being taken and may be a criminal offence.

Waste computer printed output must be disposed of with due regard to the sensitivity of the data it contains. Individual departments will be responsible for ensuring that appropriate arrangements are made.

2.5 PASSWORD SECURITY

Personal passwords must not be disclosed to anyone.

The use of another person's password to gain access to any system is not allowed.

Computers and other related equipment should not be left logged on when unattended.

Passwords should be changed every 30 days and be complex in nature where possible the Computer Operating system will enforce this.

The following should be borne in mind when creating a password:

- **DON'T** use your login name as part of your password.
- **DON'T** use initials, names, dates, or whole words associated with yourself.
- **DON'T** write your password down.
- **DON'T** 'toggle' between the same two or three passwords.

2.6 SECURED AREAS

Heads of Departments are responsible for the security of computer equipment and software within their departments.

Special care should be exercised in Area Sub Offices or other higher risk locations. Portable equipment should **NOT** be left 'lying around' on office desks.

The issue of keys to such areas should be strictly controlled and a record of all key holders maintained.

Where combination or card locks are used, they should be similarly recorded.

The transfer of keys, cards or access codes to another person is not allowed.

2.7 GENERAL

If you leave the employment of the Council you must return on or before your last working day, all identity cards, keys, manuals, Mobile Phones, equipment and any other property belonging to the Council.

You should report violations of this Security Policy to your Service Unit Manager or Head of Department

The requirements contained in this Policy are of a general nature covering all IT equipment. Additionally, there may be requirements designed for specific applications, equipment or sites.

Periodic checks will be made by Computer Department Officers and Audit Services to ensure compliance with these rules, although ultimately the responsibility for security rests with the Head of Department.

These requirements may be changed from time to time in response to changing demands, both operational and legislative. If this happens you will receive a copy of the revision.

3.0 IMPLEMENTATION AND COMPLIANCE

3.1 IMPLEMENTATION

This policy will initially be implemented through the Chief Executive and Corporate Directors of the Council.

A memo will be sent to all HOD's and SUM's to make them aware of the policy.

It is the responsibility of managers to ensure that new staff receive information about this Policy, and should be part of any local induction where appropriate. Human Resources will add the Policy to its list of policy issues provided to any new starters. Managers must also ensure that any changes to this policy are effectively communicated within their areas of responsibility.

3.2 COMPLIANCE

Managers are responsible for ensuring that staff are aware of the location of this policy. In addition, Managers are responsible for keeping staff up to date about any changes within the policy.

All staff are obliged to adhere to this Policy.

4.0 EQUALITY IMPACT ASSESSMENT

An equality impact assessment has been undertaken for the suite of policies relating to data security.

The result of this assessment shows low relevance in relation to specific equality issues and factors.

The full assessment can be found at:

[I:\Equality & Diversity\EIA\Equality Impact Assessments\Gov Connect\data security EIA.doc](#)

5.0 HEALTH AND SAFETY

There are no health and safety implications with this policy.

6.0 REFERENCE DOCUMENTS

This Policy should be read in conjunction with the following legislation, regulations and Council policies:

- COCO security checks
- Data Handling and Security Breaches
- System Access and Passwords
- Internet Security
- Email Usage
- Using Removable Media
- Contractors / Suppliers connecting to the GYBC network
- Taking GYBC computer equipment abroad

7.0 DISTRIBUTION

This Policy will be available for all the Council's designated locations. Copies will also be available from the 'I' drive and on the Council's Intranet.

8.0 REVIEW

This Policy will be reviewed on an annual basis with the next review date being April 2012.

APPENDIX A

The Data Protection Act

RELEASING INFORMATION TO PREVENT OR DETECT CRIME

This practice note (taken from guidance from the Information Commissioner's Office) explains what you need to consider when you are asked to release personal information because it is needed to prevent or detect a crime, or catch and prosecute a suspect.

Does the Data Protection Act 1998 stop me from releasing this personal information?

No. There is an exemption in the Data Protection Act 1998 (the Act) that allows you to give out personal information for these purposes (**Section 29 – Crime and Taxation**), but there are limits on what we can release.

Who might ask me to release personal information under this exemption?

The police are most likely to ask you to release personal information under this exemption. However, you may get requests from other organisations that can rely upon this exemption because they have a crime prevention or law enforcement function, for example, the Department for Work and Pensions – Benefit Fraud Section. For the sake of clarity, in this note we will continue to refer to releasing information to the police.

What personal information can I release under this exemption?

The exemption does not cover the disclosure of all personal information, in all circumstances. It only allows you to release personal information for the **stated purposes** and only if **not releasing it would be likely to prejudice (that is, significantly harm) any attempt by police to prevent crime or catch a suspect.**

What questions can I ask?

For every request for personal information we receive (and about each separate individual), we need to ask the following questions:-

- Am I sure the person is who they say they are? (for this reason particular care should be taken if the request is made over the telephone).
- Is the person asking for this information doing so to prevent or detect a crime or catch or prosecute an offender?

- If I do not release the personal information, will this significantly harm any attempt by the police to prevent a crime or catch a suspect? (The risk must be that the investigation may very well be impeded).
- If I do decide to release personal information to the police, what is the minimum I should release for them to be able to do their job?
- What else (if anything) do I need to know to be sure that the exemption applies? For example, Why is it necessary for us to provide this personal information – can they get it from another source? Or how will this personal information assist your attempts to prevent a crime or catch a suspect.

Do we have to release the personal information requested?

It is understood that most people will want to help the police to prevent crime or catch a suspect, but it is up to you to decide to release personal information under this exemption. If there are real concerns about supplying the information due to confidentiality then the police may have to come back with a court order requiring the release of the information. If the court decides you should release the information, you will not break the Act by obeying the order.

General advice

The police will, if asked, supply a form requesting the information and the reason it is required. This will be signed by an officer of the rank of inspector or higher. It is recommended that this is requested in all cases.

A record must be kept of any request and information supplied. This will be kept by the FOI team all requests must be sent to them to be logged.

If you receive a request and are unsure on how to proceed you must contact the Policy and Information Manager.

APPENDIX B

The Computer Misuse Act

The Computer Misuse Act recognises three criminal offences:

- unauthorised access;
- unauthorised access with criminal intent; and
- unauthorised amendment or damage to data.

The first offence covers simple hacking, and the second covers unauthorised access to assist in the perpetration of a more serious crime, for example fraud or blackmail. The third offence covers, among other things, the introduction of viruses and timebombs.

The maximum penalty for these offences is a fine (£2,000 in the case of simple hacking) or five years in prison (six months in the case of simple hacking).

This Act will enable victims to take legal action against their attackers (assuming that they know they have been attacked and that they can prove that their attacker knew that what they were doing was unauthorised). However, it does not excuse computer users from taking all reasonable precautions to prevent an attack in the first place.