Comisiwn y Cynulliad
Assembly Commission

NAFWC 2007 (Paper 7A)

Security Classification (if required): None
Date: Wednesday 20 June 2007
Time: 9.30-12.00
Venue: Conference room 22
Author name and contact number: Corporate Unit

ASSEMBLY COMMISSION POLICIES

Purpose and summary of issues

1. A number of Commission policies were previously agreed by the Shadow Commission (Annexes 1 – 6). Some have been modified but only to take account of the new structure being put in place by the Chief Executive. Annexes 7 and 8 were considered and agreed by the Executive Board at its meeting on 11 June 2007. The Commission is invited to endorse the policies formally.

Recommendations (including priority deadline)

2. That the Assembly Commission ratifies the following policies:

- Annex 1 – Health and Safety Policy Statement;
- Annex 2 – Staff Code of Conduct;
- Annex 3 – Public Interest Disclosure;
- Annex 4 – Procurement;
- Annex 5 – Financial Standards;
- Annex 6 – ICT Security Policy;
- Annex 7 – Code of Practice on Public Access to Information;
- Annex 8 - Data Protection Policy Statement

Discussion

3. A number of the policies were previously shared with WAG, these have since been modified to reflect the new organisation. The policies were agreed by the Shadow Commission and need to be endorsed formally by the Assembly Commission.

Governance Matters

Financial implications

4.

- Annex 1 - There are no financial implications arising from the adoption of the revised statement, over and above those inherent in the existing arrangements.

- Annex 2 – There are no financial implications arising from the introduction of the Code.

- Annex 3 – There are no financial implications arising from the adoption of the Policy.

- Annex 4 – This policy provides guidance on procurement for the Commission and its staff and is an essential part of the financial framework

- Annex 5 – These standards set out the overarching standards for financial management in the Commission and are an essential part of its governance framework.

- Annex 6 – There are no financial implications arising from the introduction of the Policy.

- Annex 7 - There are no financial implications arising from the adoption of the Code.

- Annex 8 – The only financial implication arising from the adoption of the statement is the data processing notification fee, currently £35 per annum and this cost will be met from the Corporate Unit budget.

Risk Assessment

5. All of these policies and standards are an integral part of the Commission's governance framework and, when in place, are also intended to assist in the management of risk.

Compliance

6.

- Annex 1 – Section 2(3) of the Health and Safety at Work etc Act (HASAWA) 1974 requires the Assembly Commission, as an employer, to prepare a written statement of general policy with regard to the health and safety of employees and the organisation and arrangements for carrying out that policy.

- Annex 2 – There are no compliance issues.

- Annex 3 – The Commission needs to have appropriate arrangements in place to comply with the Public Interest Disclosure Act 1998. The Act protects workers from

detrimental treatment or victimization from their employer if, in the public interest, they disclose wrongdoing.

- Annex 4 – This is a compliance document against which future procurements will be assessed.

- Annex 5 – This is a compliance document that specifies the Commission's expectations in respect of the financial management of the organisation;

- Annex 6 – There are no compliance issues.

- Annex 7 – the Lord Chancellor's Code of Practice on the Discharge of Public Authorities' Functions under Part 1 of the Freedom of Information Act 2000 states that public authorities should publish their procedures for dealing with requests for information.

- Annex 8 – The Data Protection Act does not require a data controller to issue a policy statement but the Information Commissioner identifies the training of staff on their responsibilities as good practice.

Annex 1

NATIONAL ASSEMBLY FOR WALES COMMISSION
HEALTH AND SAFETY POLICY STATEMENT

The Health and Safety at Work etc., Act 1974 imposes a statutory duty on employers to ensure in so far as is reasonably practicable the health and safety of their employees whilst at work. This duty also extends to others who may be affected by that work.

Employees also have a statutory duty to take care of themselves and others who may be affected by their acts or omissions.

To enable these duties to be carried out in accordance with current applicable legislation, it is our intent to ensure that responsibilities for health and safety matters are effectively assigned, accepted and fulfilled at all levels within our organisational structure.

1. We will, so far as it is reasonably practicable, ensure that:

- adequate resources are provided to ensure that proper provision can be made for health and safety
- risk assessments are carried out and periodically reviewed
- systems of work are provided and maintained that are safe and without risks to health
- arrangements for use, handling, storage, and transport of articles and substances for use at work are safe and without risks to health
- all employees are provided with such information, instruction, training and supervision as is necessary to secure their safety and health at work and the safety of others who may be affected by their actions
- where appropriate, health surveillance will be provided for employees
- the provision and maintenance of all plant, machinery and equipment is done so safely, and without risk to health
- the working environment of all employees is safe and without risks to health and that adequate provision is made with regard to the facilities and arrangements for their welfare at work
- the place of work is safe and that there is safe access to and egress from the work place
- monitoring activities are undertaken to ensure standards are being met as we strive to continually improve our health and safety performance.

2. It is the duty of all employees at work:

- to take reasonable care for the health and safety of themselves and of other persons who may be affected by their acts or omissions at work and co-operate with us in fulfilling our statutory duties

- not to interfere with or misuse anything provided in the interest of health and safety.

3. General:

- this Health and Safety Policy will be reviewed at least annually, amended and updated as and when necessary. Communication of any such changes will be made to all employees
- there are established and maintained effective procedures for consultation and communications between all levels of management and employees on all matters relating to health, safety and welfare
- detailed reference information for employees can be found on the Health and Safety Intranet site or from the Health and Safety Adviser.

Signed ……

Position - CHIEF EXECUTIVE …….

Date ……

POLICY STATEMENT 2007

Annex 2

Final

National Assembly for Wales Commission

STAFF CODE OF CONDUCT

FOREWORD

This Code describes the standards of behaviour required of all members of staff of the National Assembly for Wales (employees of the Assembly Commission).

As an employee of a democratically elected institution you are expected to behave in a way that will not bring the National Assembly for Wales or the Assembly Commission into disrepute or cause embarrassment to them.

As an employee of the Assembly Commission you must ensure that you perform your duties and responsibilities with honesty and impartiality at all times.

By adhering to this Code, you will ensure that you maintain the standards of integrity, conduct and concern for the public interest that each and every one of us supporting the National Assembly for Wales is required to demonstrate in our work.

The Code sets out the Assembly Commission's expectations of you as a member of staff and you should read the Code and ensure that you remain familiar with the standards of behaviour expected of you.

Not only must you ensure that you maintain the proper standards of behaviour expected of you in your every day work, but you must not place yourself in a position where others might have reasonable cause to question your behaviour.

If you are ever uncertain as to what is expected of you in terms of behaviour you must seek advice from your line manager.

If you have reason to believe that this Code has been breached or is in danger of being breached, then you have a responsibility to bring this to the attention of management.

If you believe that you are being required to act in a way which conflicts with this Code, you should talk to your line manager or Human Resources.

If you have raised a matter and you do not receive what you consider to be a proper response, then you should report the matter to me.

Claire Clancy

Chief Executive of the Assembly Commission and Clerk of the National Assembly for Wales ("Chief Executive and Clerk")

May 2007

About the Code of Conduct

1. This Code forms part of your terms and conditions of employment and part of the legal contract between you and the Assembly Commission. It sets out the standards of behaviour expected of you which follow from your position in serving the Assembly.

Accountability

2. The person or body from whom you need to seek permission where specified in this code is:-:

- Team Support to Band G - Director
- Director - Chief Executive and Clerk
- Chief Executive and Clerk - Assembly Commission

Principles

3. You must serve the National Assembly for Wales in accordance with the principles[1] set out below.

- ***Selflessness*** – You must not take decisions or give preferential treatment to any individual or organisation in order to further your private interests and so compromise the performance of your role.
- ***Integrity*** – You must not place yourself under any financial or other obligation to outside individuals or organisations that might influence you in the performance of your official duties.
- ***Objectivity –*** You must provide information and advice, including advice to elected members and committees on the basis of evidence, and in a way that accurately reflects the options and facts, taking due account where appropriate of professional advice. You must serve the National Assembly for Wales and the Assembly Commission to the best of your ability irrespective of your own political beliefs. You must refrain from political activity and campaigning which could call into question your impartiality and ability to serve all elected members equally.
- ***Accountability*** – You must work to the best of your ability to support the implementation of the decisions of the National Assembly for Wales and the Assembly Commission and be prepared to be accountable for your actions and submit yourself to scrutiny as appropriate to your office.
- ***Openness*** – You must be as open as possible about the decisions and actions you take and be prepared to give reasons for your decisions.

[1] *The Nolan Committee produced the report on Standards in Public Life in May 1995 at the request of the Prime Minister. The Committee investigated standards in British public life and as a result, produced The Seven Principles of Public Life.*

- ***Honesty*** - You must not solicit or accept money, gifts, favours or hospitality from others or any other benefits that might be construed as compromising your integrity.
- ***Leadership –*** You should promote and uphold these principles by leadership and example.

Rules

4. You will find the conduct rules in the following Sections:

(For full and detailed information on these sections, please refer to the Terms and Conditions of Service document and the related Policies and Procedures)

Section 1 Propriety (appropriate behaviour)

Section 2 Confidentiality and official information

Section 3 Outside occupations and appointments

Section 4 Participation in political activities

Section 5 Other rules

Breach of conduct rules

5. If you breach any of the conduct rules, or if through negligence on your part other people breach these rules, you may be subject to disciplinary action as laid out in the disciplinary policy.

More information

6. If you wish further advice about the conduct rules, you should contact Human Resources.

Section 1 Propriety

Arrest or conviction on civil or criminal charges

7. You must, as soon as practicable inform your line manager if you are arrested, refused bail or convicted of any criminal offence. This does not apply to traffic offences unless the possible penalty includes imprisonment or disqualification from driving or

involves an official vehicle. Failure to inform will be considered an act of gross misconduct.

Unlawful activity

8. You have a duty to comply with the law; including international law and treaty obligation and to uphold the administration of justice and to report any evidence of unlawful and criminal activity. The Assembly Commission's Public Interest Disclosure Policy provides guidance on the reporting arrangements.

Bankruptcy and insolvency

9. If you are bankrupt or declared bankrupt by a court of law you must report this fact as soon as practicable to your line manager and the Chief Executive and Clerk. Failure to disclose bankruptcy and insolvency will be considered an act of gross misconduct.

Acceptance of money, gifts, rewards and hospitality

10. You must not accept any money, gifts, hospitality, award, decoration, or other benefit from any member of the public or organisation with whom you have been in contact through your official duties. This does not apply to isolated gifts of a trivial nature, for example a diary, calendar or modest hospitality, provided that it is not a regular occurrence. If the refusal of such a gift is likely to cause offence to the giver, you should report the facts immediately to your line manager.

11. A register of money, gifts and hospitality is maintained and if you are offered money, gift or hospitality (even if you do not accept it) you must ensure that the offer is entered on the register (the keeper of the register will need to know the nature of the gift or hospitality, whether you accepted it, who offered it, why it was given and an estimated value). Your line manager can inform you of the procedure for registering such money, gifts and hospitality. You should take advice from your line manager before you accept any money, gifts and hospitality about which you have any concerns.

12. If you are found to have accepted or have failed to register the receipt of money, gifts, hospitality, benefit or any other consideration in circumstances where it conflicts with your official duties, this will be considered to be an act of gross misconduct.

Receipt of fees

13. Any fees received from an outside source must be paid to the Assembly Commission, if the payment is for services which form part of your official duty. In circumstances where all or part of the work involves private as well as official time or if the official time is made up, you may make an application to your line manager for permission to retain all or part of the fee as appropriate. In accordance with section 3 of this Code, you must seek permission before accepting any outside employment which might affect your work directly or indirectly.

Political influence

14. You must not use your position and proximity to elected members and external public bodies to gain support or influence for your own personal benefit. This does not preclude you from approaching your Assembly Member through the normal channels of correspondence and surgeries.

Contracts for goods and services

15. Unless you have obtained permission from your line manager, you should not let Assembly Commission contracts to:

- your immediate family, close personal friends and business associates;
- any company or partnership for which your immediate family, close personal friends and business associates may work;
- any employee of the Assembly Commission or their immediate family or any organisation of which an employee or a member of the their immediate family is a Partner or Director;

16. Where permission is granted, you must still register the decision and acquaint the Assembly Commission's Procurement Officer of the background before proceeding.

Section 2 Confidentiality and official information

17. Misuse of confidential information breaches the duty of confidentiality owed to the National Assembly for Wales and to the Assembly Commission and will be considered an act of gross misconduct.

18. Whilst information obtained in the course of your employment should be treated as confidential, you should be aware that information which you process may be released to individuals or into the wider public domain in accordance with legislation and the Assembly Commission's policies on access to information. You must not make unauthorised use of confidential information either during or after your period of employment. You are required to treat personal information (this applies to all forms of data about an individual, including paper documents, databases and emails) confidentially and in line with the Data Protection Policy operated by the Assembly Commission and in accordance with the Data Protection Act 1998.

19. Assembly Commission employees, who were previously Civil Servants and notified that they were subject to the Official Secrets Act, will continue to be bound in respect of information etc. which came into their possession whilst a Civil Servant. Such employees will be expected to comply with their duties under this Act and breach of their duties will be considered a potential breach of the Code. Assembly Commission employees who have never been subject to the Official Secrets Act will not be subject to the provisions of the Act.

General rules

20. No confidential official information may be disclosed by you without permission as set out in paragraph 2 above.

21. Information, confidential or otherwise, to which you have had access, must not be used to frustrate the policies or decisions of the National Assembly for Wales or the Assembly Commission.

22. You must seek permission as set out in paragraph 2 above for any activities involving the following that are not undertaken as part of your official duty:

- participation in any media broadcast (sound or vision) regarding the business of the National Assembly for Wales / Assembly Commission;

- publication or broadcasting of any personal memoirs relating to work carried out for the National Assembly for Wales / Assembly Commission;

- dissemination of any information (verbal or written) which is passed to any journalist for publication relating to the National Assembly for Wales / Assembly Commission;

- participation in any opinion poll or market research survey relating to attitudes or opinions on political matters;

- any arrangements regarding the publication of articles or materials which have been produced by you as part of your official duties, copyright of which will be owned by the Assembly Commission pursuant to the Copyright Designs and Patents Act 1988.

23. The above does not preclude national, organisational or branch representatives of a recognised trade union from discharging their duties as representatives.

Section 3 Outside occupations and appointments

Outside occupations

24. You must seek permission as set out in paragraph 2 above before accepting any outside employment.

25. You may not:

- at any time, engage in any private activity which would require your attendance during working hours or in any way tend to impair your usefulness as an employee of the Assembly Commission, unless you have been given permission as set out in paragraph 2 above to do so;

- engage in any occupation or other activity which might in any way conflict with the interests of the National Assembly for Wales or the Assembly Commission or be inconsistent with your position as an employee of the Assembly Commission;

- engage in any outside activity involving payment that uses experience or knowledge acquired during the course of official duties, without obtaining consent as set out in paragraph 2 above;

- hold a directorship or undertake executive work in a private company, firm or other organisation or engage in consulting work which has a connection with your official duties or is on behalf of a firm or concern which is in contractual or other special relationship with the National Assembly for Wales and or the Assembly Commission, without first obtaining consent as set out in paragraph 2 above.

26. If you have any doubt about the propriety of any personal private activity, you should seek further guidance.

Appointments to public boards

27. If you wish to accept an appointment to any public board or body financed wholly or in part from public funds, you must seek consent as set out in paragraph 2 above.

Acceptance of outside appointments

28. It is considered to be beneficial for all concerned that the skills and experience of those working for the Assembly Commission are able to transfer to the wider community and as a result, most applications submitted under these rules are approved without condition.

29. The aim of these rules is to maintain public trust in the people who work for the Assembly Commission and in particular:

- to avoid any suspicion, no matter how unjustified, that the advice and decisions of staff might be influenced by the hope of future employment with a particular organisation;

- to avoid the risk that a particular organisation might gain an improper advantage over competitors by employing someone who, in the course of their employment with the Assembly Commission has had access to technical or other information which those competitors might legitimately regard as their own or to information relating to proposed developments in the Assembly Commission's policy which may affect the organisation or its competitors.

30. You are required to obtain permission as set out in paragraph 2 above before accepting, within two years of resignation or retirement or otherwise leaving the employment of the Assembly Commission, any offer of employment in business and other bodies including overseas governments and consultancy work, whether on an employed or self employed basis and whether full time, part time or fee paid.

Section 4 Participation in political activities

Impartiality

31. For you to serve all elected members equally, it is essential that the National Assembly for Wales and the public have confidence that your personal views do not affect the discharge of your official duties. The aims of the rules set out below, are to allow you the greatest possible freedom to participate in public affairs without infringing this fundamental principle. *(It should be noted that the Government of Wales Act 2006 disqualifies a member of staff of the Assembly Commission from being an Assembly Member).*

General rules applicable to political activity

32. The following rules apply to you at all times:-

- you cannot take part in any political activity whilst on duty or in uniform or on Assembly Commission premises;

- you must not attend outside conferences or functions convened by or under the auspices of a party political organisation in your official capacity;

- care must be taken to avoid any embarrassment to the Assembly Commission or the Assembly by you bringing yourself prominently to public notice in party political controversy as an employee of the Assembly Commission;

- you must ensure that your personal political views are expressed with moderation so as not to inhibit or appear to inhibit loyal and effective service to members of another party.

Restrictions

33. You may not take part in political activities relating to the National Assembly for Wales, although you may seek permission as set out in paragraph 2 above to take part in other political activities. In considering such requests, the degree of contact you have with Assembly Members in the discharge or your official duties will feature heavily.

34. For the purpose of these rules, “political activities” are defined as follows:

35. At national level within Wales

- announcement of your candidature for membership of the National Assembly for Wales;

- holding office (other than membership) in a party political organisation, office which impinges wholly or mainly on the party politics in a field relating to the National Assembly for Wales;

- canvassing on behalf of a candidate for the National Assembly for Wales;

- contributing to articles for publication, books or submitting letters to the press relating to debates on controversial political issues within the National Assembly for Wales;

- speaking in public on matters of national political controversy*.

36. At a national level in the rest of the UK

- announcement of your candidature for the House of Commons, the Scottish Parliament, the Northern Ireland Assembly or the European Parliament;

- holding office (other than membership) in a party political organisation, office which impinges wholly or mainly on the party politics in a field of the House of Commons, The Scottish Parliament, the Northern Ireland Assembly or the European Parliament;

- canvassing on behalf of a candidate for the House of Commons, The Scottish Parliament, the Northern Ireland Assembly or the European Parliament;

- contributing to articles for publication, books or submitting letters to the press relating to debates on controversial political issues;

- speaking in public on matters of national political controversy*.

37. At local level

- candidature for local authorities;

- holding office (other than membership) in a party political organisation, office impinging wholly or mainly on party politics;

- canvassing on behalf of candidates for election to local authorities or a local political organisation;

- contributing to articles for publication, books or submitting letters to the press relating to debates on controversial local political issues;

- speaking in public on matters of local political controversy[2].

Section 5 Other rules

[2] This should not preclude national, organisational or branch representatives of a recognised trade union from discharging their duty as representatives.

38. You must not bring the Assembly Commission into disrepute by publicly making derogatory, adverse or objectionable comments regarding individuals (whether officials, Members or others) or organisations or participate in any activities which conflict with the interests of the National Assembly for Wales.

Annex 3

PUBLIC INTEREST DISCLOSURE

CONTENTS

THE POLICY

Annex

THE POLICY

Aims of the policy

1. This Policy has a twofold aim:

   - to encourage the reporting of matters of proper concern

   - while protecting employees and the National Assembly for Wales Commission from unfounded and malicious allegations.

2. The best way to achieve these two aims is to put in place **fair and flexible internal procedures** so that concerned staff never feel forced to turn to an external body and staff named in mistaken allegations are not exposed to public criticism.

3. This Policy has been agreed between the Management and Trade Union Sides. The Trade Unions support in full the aims of the Policy and the supporting procedures set out below.

BACKGROUND

4. Under the terms of the Assembly Commission's Code of Conduct for Staff (the Code)[1] staff are **required** to report evidence of criminal or unlawful activity. The Code also says that you **may** report other breaches of the Code committed by colleagues.

5. We **encourage** staff to report **any** suspected wrongdoing. Staff members who report a genuine concern, even if it turns out to be mistaken, are doing their duty as public servants. They will not be disciplined or subjected to any other detriment. On the contrary – if a staff member fails in his or her duty to report suspected criminal or unlawful activity, that failure could lead to disciplinary action.

6. This Policy applies to all members of staff of the Assembly Commission. However, we recognise that it can be difficult for staff members to report concerns about colleagues or senior staff. This Policy is designed to address those difficulties and to reassure staff that they can expose wrongdoing without any risk to themselves. You may raise your concerns with your manager including the Chief Executive and Clerk (see paragraphs 9 and 10).

   Parliament has recognised the need to protect employees who raise concerns in the public interest – often referred to as "whistleblowers". The Public Interest Disclosure Act 1998 ("PIDA"), in fore since July 1999, was enacted for this purpose. The main provisions of PIDA are set out in Annex 2 to this Policy. Many of the disclosures potentially protected by

   the Act corresponds to disclosures about breaches of the Assembly Commissions Code of Conduct for staff, but PIDA also covers disclosures about two specific areas which might not spring to mind under the code: danger to health and safety and damage to the environment.

WHAT IS MEANT BY PUBLIC INTEREST DISCLOSURE IN THIS POLICY?

7. In this Policy, "public interest disclosure" means a member of staff reporting suspected wrongdoing, or an attempt to cover up wrongdoing, on the part of a Assembly Commission employee or another party acting on behalf of the Assembly Commission (such as a contractor).

   It will also apply to the Assembly Commission, but in this context the reference to the Assembly Commission means the Assembly Commission exercising its powers through members of staff. This does not include the acts or omissions of Assembly Members acting as individuals or in their individual capacity as Assembly Members.

   "Wrongdoing" is not a technical term. We want to encourage staff to report any genuine concern they may have, without worrying about technical definitions

WHAT TO DO IF YOU SUSPECT WRONGDOING

8. You should first report the issue, orally or in writing, to your line manager, if possible. However, if you feel unable to go to your line manager, for whatever reason, you can raise it with any of the following persons:

   - Your Director
   - The Head of Finance
   - The Head of HR
   - The Commission's Head of Security

9. If you feel unable to go to any of the persons listed above, or feel that the issue is so serious that it has to be reported directly to the highest levels, you can contact, orally or in writing, the Chief Executive / Clerk.

10. If you prefer, instead of contacting one of the persons listed above, you may request your Assembly Commission recognised trade union or professional association to raise a matter with one of them on your behalf. Your recognised union or professional association can also provide you with advice on how to take your concern forward**.**

11. Alternatively, you can seek advice from one of the Assembly Commission's Nominated Officers (see paragraph 19).

12. You will not be disciplined or subjected to any detriment on the grounds that you did not choose the most appropriate person from the above list. The important thing is to raise your concern with one of them.

13. You will not be expected to prove that an allegation is true (but see paragraph 17).

14. You may be worried that this is not the right policy to use to raise your concern. Don't be. The important thing is to raise it (in accordance with paragraphs 9 to 12). This policy is designed to ensure that the correct procedure is followed from then on. For your information, the other policies and procedures which may be relevant are listed in Annex 1.

THE CHIEF EXECUTUVE / CLERK'S UNDERTAKINGS TO YOU

15. Provided that you raise a concern in good faith, and follow the procedures set out in this Policy:

- You will not be disciplined or subjected to any other detriment to your career as a result, even if the concern turns out to be mistaken

.

- Your identity will be kept confidential for as long as you require, while this is under the Assembly Commission's control[2], subject to the requirements of criminal investigations, where applicable. (More detailed provisions as to confidentiality and anonymity are set out in paragraphs 29 to 34).

- The Chief Executive and Clerk will take all other reasonable steps to protect you from harassment or other personal detriment.

- You will be informed of the action being taken in response to your concern and of the outcome (subject to any legal constraints). More detail of this commitment is given in paragraphs 24 to 28).

The Assembly Commission has a duty to protect members of staff and the organisation itself from unfounded or malicious allegations. Malicious allegations, and allegations made without any grounds at all, will be treated as a serious disciplinary matter, which could result in dismissal. You should note that PIDA will not protect you if you make such allegations. The matter will be viewed with even greater seriousness if the allegation is made externally.

16. Where an allegation is found to be mistaken or groundless, we will take all reasonable steps to protect any person implicated in it from adverse consequences.

WHAT THE NATIONAL ASSEMBLY FOR WALES COMMISSION WILL DO IN RESPONSE TO A CONCERN RAISED UNDER THIS POLICY

17. The Nominated Officers for the purposes of this Policy are (to be determined). They must:

- keep a record of all matters raised under the policy and of the action taken; and

- carry out the commitment to inform the individual raising the concern of the action taken in response to their concern (paragraphs 24 to 28).

18. As soon as a concern is reported under this Policy to any of the people listed in paragraphs 9 and 10, that person must refer the matter to one of the Nominated Officers and must inform the individual raising the concern that they are doing so. (See paragraph 43 for concerns implicating Nominated Officers).

19. If it appears necessary to take interim measures urgently – for instance, to protect public funds – this will be done immediately, before any inquiries or investigation process.

20. Otherwise, the first step will be to hold informal initial inquiries, to determine the most appropriate form of investigation (if any) and the most appropriate process for the consideration of the concern. Concerns that fall more appropriately within the scope of other formal procedures, such as the grievance procedure, will be referred for consideration under those procedures.

21. If it is decided that an investigation is necessary, the concern will be rigorously investigated by persons who are not implicated and who are independent of those implicated. This may be done by members of management or the disciplinary process, as considered appropriate. Matters may also be passed to the police for investigation.

22. Where a concern is referred to the Nominated Officers under paragraph 20, they will act as a point of contact with the individual raising the concern (or other person reporting the matter on behalf of the individual, such as a trade union representative) until the Senior Management of the Assembly Commission considers the matter as resolved.

23. All communications in writing between the Nominated Officers and the individual raising the concern will be made under confidential cover.

24. Within 10 working days of the concern being drawn to the attention of the Nominated Officers, they will write to the individual raising the concern (or other person reporting the matter on behalf of the individual under paragraph 11:

    - acknowledging the report or referral of the concern

    - giving an indication of how the Assembly Commission proposes to deal with the matter and

    - indicating the likely time-scale for providing a final response.

    If it is impossible to give the indications within 10 working days, the letter will say so, giving reasons, and the indications will be given as soon as possible thereafter.

25. If a decision is made not to investigate the concern, this will be notified to the individual raising the concern, in writing, as soon as possible and within 10 working days at the latest.

26. The individual raising the concern will be given as much information as possible on the outcome of the investigation. However, there may be constraints because of the Assembly Commission's duties of confidentiality or fairness or other legal considerations.

CONFIDENTIALITY AND ANONYMITY

27. As stated in paragraph 16, the Chief Executive and Clerk undertakes to keep the identity of the individual raising the concern confidential for as long as he or she wishes and as long as the matter remains under the Assembly Commission's control. The only exception to this is that we reserve the right to reveal the individual's identity to the police if this is necessary for the proper investigation of a suspected criminal offence. In that case, the Nominated Officers will inform the individual that his or her identity is to be revealed to the police, and will take all reasonable steps to protect him or her from harassment or other personal detriment (except where he or she is charged with a criminal offence – for instance, where an individual makes a false allegation to distract attention from his or her own criminal conduct).

28. Any member of staff who reveals the individual raising the concerns identity in breach of this Policy will face disciplinary action, up to and including dismissal.

29. However, keeping the identity confidential may make it more difficult to carry out a full investigation into the matter or to take action against a wrongdoer. If we consider that it is not able to resolve the concern without revealing the individual's identity (other than to the police, where necessary, as stated above) we will discuss with the individual whether, and how, to proceed.

30. All concerns expressed anonymously will be considered and will be investigated further if the Nominated Officers consider it appropriate and worthwhile to do so. Concerns raised anonymously are often difficult to investigate properly and this is a factor the Nominated Officers will take into account. Moreover, if a concern is raised anonymously, the individual raising the concern may not benefit from the protection set out in paragraph 16. The Nominated Officers will therefore always ask the individual raising the concern to give their name. The confidentiality provisions set out in paragraphs 29 to 31 will then apply.

31. It is easy to make malicious or unfounded allegations anonymously. The initial inquiries into anonymous allegations will therefore be handled with particular sensitivity.

32. In disciplinary proceedings against a member of staff accused of making a malicious or unfounded allegation against a colleague under this Policy, the fact that the allegation was made anonymously will be an aggravating factor.

IF YOU ARE NOT SATISFIED WITH THE WAY YOUR CONCERN HAS BEEN DEALT WITH

33. If you have raised a concern under this Policy and are dissatisfied with the way in which it is being handled, you can report your dissatisfaction to another of the persons listed in paragraphs 9 or 10. That person will be required to respond to it as a fresh concern raised under this policy. If you and the Nominated Officer both agree, that person may also take over responsibility for responding to your original complaint.

DISCLOSURES TO REGULATORS AND OTHER EXTERNAL DISCLOSURES

34. The aim of the Policy is to make our procedures so fair and flexible that you will never feel forced to raise a concern with an external body. However, PIDA recognises that, in certain circumstances, an employee may be justified in such action. More detail about this is given below and in Annex 2.

Regulators

35. There are certain legal protections if you go to a body prescribed under PIDA. The list can be obtained from (to be determined). It includes bodies such as the Auditor General for Wales. You would only be protected if:

- **the disclosure fell into one of the PIDA protected categories**
- **you raised the concern in good faith and**
- **you reasonably believed it to be substantially true**

See Annex 2 for details.

Other external disclosures

36. Raising a concern outside the Assembly Commission instead of using the procedures set out in this Policy, and in certain circumstances even after doing so, is a serious disciplinary offence which could result in dismissal, unless your action is protected by PIDA. That protection will only be available in exceptional cases. More details are set out in Annex 2 to this Policy.

37. In addition, the Assembly Commission's Terms and Conditions of Service Code and the Staff Code of Conduct require that members of staff do not disclose confidential information without proper authority. In considering taking a concern to an unapproved organisation, staff should be aware of their duty of confidentiality and ensure that no confidential information is divulged unless there are overriding public interest considerations such as to attract the protection of PIDA.

38. Finally, members of staff who are former civil servants need to consider the provisions of the Official Secrets Act 1989. Assembly Commission employees who were previously Civil Servants and notified that they were subject to the Official Secrets Act will continue to be bound in so far as information etc which came into their possession whilst a Civil Servant. Such employees will be

expected to comply with their duties under this Act and breach of their duties will be considered a potential breach of the Code. Assembly Commission employees who have never been subject to the Official Secrets Act will not be subject to the provisions of the Act. An individual raising a concern will not be protected by PIDA if, in disclosing the information, he or she commits a criminal offence – such as breach of the Official Secrets Act.

39. A member of staff who is considering making an external disclosure may wish first to seek advice from his/her trade union or legal adviser. If you do seek such advice, the adviser will need to know at least some details about the information, or the kind of information, you are considering disclosing. If you make a disclosure in the course of obtaining legal advice, you will be protected by PIDA. So be careful to reveal the information only to your legal adviser him or herself - not, for instance, to a helpline operator or in an answer phone message.

WHAT TO DO IF A CONCERN IS RAISED WITH YOU

Reports from staff

40. If a concern is raised with you internally, for example as a line manager, you must report it immediately to one of the Nominated Officers. You must then consider how to handle the matter. The Nominated Officers can advise if required. The Nominated Officers may also advise whether one of the alternative procedures/policies set out in Annex 2 may be more appropriate to your particular complaint. You will need to let the Nominated Officer know what action has been taken and/or decided on, so that an update can be provided to the individual raising the concern within 10 working days of the matter being raised.

41. Paragraph 42 will not apply to a concern that implicates all the Nominated Officers. In that case, the person to whom the concern is reported should:

- Deal with the matter in accordance with paragraphs 21 to 23 and 44 and 45 (apart from the references to Nominated Officers)
- keep the individual raising the concern regularly informed of developments, as far as possible, and
- inform the Chief Executive and Clerk that a concern implicating both the Nominated Officers has been raised.

42. In deciding how to handle the matter, you must comply with the procedures set out in paragraphs 21 to 23 and the Chief Executive / Clerk's undertakings to staff (paragraph 16). As well as consulting the Nominated Officers, you can (provided the individual raising the concern consents) consult one or more of the other persons listed in paragraphs 9 or 10. However, the number of persons informed should be strictly limited to those who need to know at each stage of the process.

43. You must pay the strictest attention to the confidentiality provisions set out in paragraphs 29 to 31. You will be responsible for ensuring that all the undertakings given to individual raising the concern are kept. The individual's identity should not

be revealed to anyone but the Nominated Officers and those who absolutely need to know for the purposes of the investigation and consequent action. Written records must preserve this confidentiality. When communicating with others about the concern, think carefully about what method will be the most secure. An example of matters you should bear in mind is the fact that many senior staff (and others) have shared e-mail inboxes.

Reports from outside the Assembly Commission

44. A member of the public or an outside body may contact the Assembly Commission to raise a concern about an employee.

45. In such instances, you should seek advice from a Nominated Officer who will decide the most appropriate course of action. Alternatively, the person raising the concern can speak directly to a Nominated Officer. It is likely that such allegations will be more appropriately dealt with under the Assembly Commission's Complaints Procedure.

MONITORING THE POLICY

46. The Nominated Officers will maintain a record of all matters raised through the Public Interest Disclosure Policy so that an assessment may be made of the effectiveness of the Policy and any emerging patterns. The Policy will be reviewed in consultation with Trade Union Side, initially after one year and thereafter every three years (or earlier if necessary to comply with new legislation).

1 Copies of the Code will be issued to all staff in May 2007 and are given to new staff as part of their induction process. Further copies can be obtained from the HR.

2 The identity of the individual raising a concern might emerge in circumstances beyond the Chief Executive / Clerk's control, for instance, in court proceedings.

ANNEX 1

PUBLIC INTEREST DISCLOSURE POLICY

Main provisions of the Public Interest Disclosure Act 1998

1. The Act does not introduce a general protection for individuals raising a concern in all circumstances. In particular, the individual will not be protected if, in disclosing the information, he or she commits a criminal offence.

2. In order to benefit from the protection of the Act and of this Policy, a disclosure must satisfy certain conditions. The first condition relates to the subject-matter of the disclosure. There is then a further set of conditions depending on who the disclosure is made to**.**

Subject-matter of the disclosure

3. The Act protects only disclosures of information which, in the individual's reasonable belief, tends to show that one of the following acts has occurred, is occurring or is likely to occur. The specified acts are:

- a criminal offence
- a failure to comply with a legal obligation
- a miscarriage of justice
- the endangering of an individual's health or safety
- damage to the environment
- deliberate concealment of information relating to any of the above.

If your belief turns out to be mistaken, you will still be protected provided that it was reasonable to think as you did.

Who the disclosure is made to

4. **Disclosure to the employer** (i.e. an internal disclosure) will be protected provided that:

- the information falls within paragraph 3 and
- the disclosure is made in good faith.

5**. Disclosure to a regulator** will be protected if:

- the information falls within paragraph 3 and
- the disclosure is made in good faith and

- the individual reasonably believes that the information and any allegation in it are substantially true.

6. **Disclosure to other external bodies** will only be protected if:

- the information falls within paragraph 3 and
- the disclosure is made in good faith and
- the individual reasonably believes that the information and any allegation in it are substantially true and
- the individual is not motivated by personal gain and
- the individual reasonably believes that the information and any allegation in it are substantially true.

7. The additional preconditions for an external disclosure to be protected are:

- The individual raising a concern must reasonably believe that they may be victimised if they raise the matter internally or with a prescribed regulator **or**
- There is no relevant prescribed regulator and the individual reasonably believes that evidence related to the disclosure they wish to make is likely to be concealed or destroyed if they raise the matter internally **or**
- The concern has already been raised with the employer or a prescribed regulator **or**
- The concern is of an exceptionally serious nature.

8. As stated in paragraph 6, it must be "reasonable" to make the disclosure in the way chosen. In assessing reasonableness, employment tribunals considering cases of victimisation or unfair dismissal arising out of concerns being raised will consider all the circumstances.

9. If the reason for turning to an external person or organisation was that the concern was exceptionally serious, an important factor for the tribunal will be the choice of person/organisation. Disclosure to the media is unlikely to be reasonable except in very unusual circumstances,

for instance where the maximum number of people need to be warned of an imminent danger. PIDA will not protect employees who contact the media in the hope of gain.

10. If the reason for making the disclosure externally is one of the others listed in paragraph 7, the tribunal will assess reasonableness in the light of and in particular:

- The identify of the person to whom the disclosure was made,
- The seriousness of the concern,
- Whether the risk or danger still exists, and
- Whether the disclosure breached a duty of confidence that the employee owed to a third party. If the employee had already raised the concern with his/her employer, the tribunal will look at whether he or she followed the internal procedures in doing so.

Annex 2

Other internal routes for raising concerns:

The Assembly Commission has a range of other policies and procedures which relate to complaints, personnel issues, integrity and operating procedures:

- The grievance procedure - which relates to individual disputes or problems
- The disciplinary procedure - which addresses cases of deviation from expected standards of behaviour.
- The fraud policy – which requires all staff to act honestly and with integrity and sets out responsibilities regarding the prevention of fraud.
- The appeals procedure relating to reports of crises of conscience
- The Code of Practice on Complaints – relating to complaints by members of the public (this is published on the Assembly Commission's Intranet site

Annex 4

OUR PROCUREMENT VALUES

a. SUSTAINABILITY

To put "sustainability" at the heart of our procurement process.

Sustainable procurement is procurement that uses our influence in ways that benefit society, the economy and the environment. It is about looking beyond short-term costs, to decisions based on whole-life costs, including social and environmental implications. We want sustainable purchases that offer good value – not cheap purchases that are unsustainable.

b. QUALITY SERVICES

To deliver the quality of services that Members, staff and the public have a right to expect.

We use procurement to deliver our services. We will work collaboratively with suppliers - establishing clear expectations and standards; working with realism; communicating openly; and balancing cost with qualitative factors.

c. COMMUNITY SUPPORT

To support community through using small & medium enterprises .

We will be socially responsible and actively encourage the participation of Small and Medium Enterprises to share the economic benefits of our procurement fairly. We will maximise access to our contract opportunities by advertising, wherever practical, via Sell2Wales.co.uk

d. VALUE FOR MONEY

To secure value for money.

We're spending tax payers' money so we don't want to be wasteful! We'll look for the best deal we can find – but not simply the cheapest. We need to balance all our Values in a way that gives us what we want, at a price that represents good value for money. This won't be a one-off event either – we'll work with our longer-term suppliers to identify efficiencies and continuous improvements to the goods and services we procure.

e. TRANSPARENCY

To act professionally, fairly, honestly and transparently.

Trust and public perceptions are important to us. We want the best deal for Wales and we'll only get it by acting in a manner that promotes the highest standards of practice.

f. ***EQUALITY***

We will ensure our procurement processes have full regard to equality.

We will comply with all relevant statutory regulations. We will incorporate, where appropriate, equality considerations in specifications and the processes for supplier appraisal, contract award and contractor performance management.

Annex 5

National Assembly for Wales Commission

Financial Standards

Introduction

These Financial Standards outline the requirements of the National Assembly for Wales Commission in respect of the management of its finances and use of resources. They are underpinned by detailed financial procedures, which provide guidance on processing transactions, management of assets and the operation of financial controls.

These Standards have been endorsed by the Commissioners and have been issued under the authority of the Chief Executive and Clerk who is also the Commission's Principal Accounting Officer. All staff and others contracted to work for the Commission are required to understand and comply with these Standards. Non-compliance may result in disciplinary action.

Interpretation

Detailed instructions on financial procedures should be interpreted by reference to these Standards. If any clarification is required, advice should be sought from the Chief Operating Officer.

The Commissioners will review these Standards from time to time taking account of any views provided by the Corporate Governance Committee and others, such as our auditors. Amendments may be made at any time if necessary – for example in response to a specific event or developments in best practice.

Roles and responsibilities

Commissioners

Section 27 of the Government of Wales Act 2006 established the Assembly Commission as a body corporate with a duty to provide to the Assembly or ensure that the Assembly is provided with the property, staff and services required for its purposes. The Commissioners are ultimately responsible and accountable to the Assembly for the governance of the Assembly Commission as a corporate body.

The Commissioners have responsibility for agreeing the annual budget prior to it being submitted for Assembly approval and for ensuring that the organisation is well managed within the resources made available. They have a key role in ensuring that the key risks to the organisation are identified and managed, and that a sound internal control framework is in place and operating effectively.

Chief Executive and Clerk

The Chief Executive and Clerk is the permanent head of staff of the Assembly Commission and, by virtue of Section 138 of the 2006 Act, its Principal Accounting Officer (PAO). The Treasury has designated the Chief Executive's responsibilities as Accounting Officer.

In particular, the PAO has personal responsibility for:

- the propriety and regularity of the public finances for which she is answerable;
- the keeping of proper records;
- prudent and economical administration;
- the avoidance of waste and extravagance; and
- the efficient and effective use of all the available resources.

The PAO must:

- sign the financial accounts and in doing so accept personal responsibility for their proper presentation in a form directed the Treasury;
- ensure that proper financial procedures are followed and that accounting records are maintained in a form suited to the management of the finances of the organisation as well as in the form prescribed for the annual accounts;
- ensure that the public funds entrusted to the Commission are properly and well managed and safeguarded;
- ensure that the Commission's assets are controlled and safeguarded;
- ensure that in considering proposals relating to the Commission's expenditure or income all relevant financial matters are taken into account, having due regard for the need to obtain value for money and any issues of propriety or regularity; and
- sign the statement on internal control published with the annual accounts

The Principal Accounting Officer is required to ensure that a sound system of internal control is maintained to support the achievement of the organisation's policies, aims and objectives; and to review regularly the effectiveness of that system. In addition, the PAO is required to ensure that managers at all levels in the organisation:

- have a clear view of the organisation's objectives, and the means to assess and, wherever possible, measure outputs or performance in relation to those objectives;
- are assigned well-defined responsibilities for making the best use of resources, including a critical scrutiny of output and value for money; and
- have the information (particularly about costs), training and access to the expert advice which they need to exercise their responsibilities effectively.

The PAO may be required to give evidence to the Assembly's Audit Committee and the House of Commons Committee of Public Accounts in respect of the Commission's

finances and use of resources. Such evidence will usually be taken on the basis of a report by the Auditor General for Wales or the Comptroller and Auditor General.

Finance Director

The Chief Executive and Clerk has appointed the Chief Operating Officer as the Finance Director of the Assembly Commission. The Finance Director's responsibilities are detailed in Chapter 4 of Government Accounting and can be summarised as providing the Accounting Officer with appropriate and timely advice, information, support and assurance in some or all of the following key areas:

- developing the Commission's aims and objectives;
- establishing the Commission's planning mechanisms, so as to provide a realistic assessment of the resources required by the Commission and of how these resources will be provided;
- determining the allocation of resources to the strategic and business plans of each area of the Commission, so that proper account is taken of agreed Commission priorities;
- assessing the competing priorities between constituent areas of the Commission so that conflicting demands for resources arising within the Commission can be resolved;
- monitoring the outturn of performance and resource consumption against plan, so that timely corrective action can be implemented as required;
- scrutinising the Commission's performance-management system in order to achieve maximum value from the pay bill; and
- ensuring that the Commission's staff take account of accepted standards of regularity and propriety and the need to secure value for money.

Corporate Governance Committee

The Commissioners have established a Corporate Governance Committee to support the Principal Accounting Officer by offering objective advice and providing assurance on issues concerning the risk, control and governance of the Commission. It has no executive authority in its own right, over the operations of the Commission or the internal and external auditors. However, it advises the PAO on the adequacy, and the appropriateness in the light of both known and emerging risks, of the work plans of those bodies. It also advises the PAO on the annual accounts (including the Statement on Internal Control) and on the adequacy of management's responses to the findings and recommendations made by the internal and external auditors.

Internal audit

The role of the internal auditors is to provide independent and objective advice to the PAO on the operation of internal controls and the arrangements for the identification and management of risk. The Head of Internal Audit has the right of direct access to the PAO and the Corporate Governance Committee where necessary.

Internal Audit is required to comply with the Government Internal Audit Standards. Its plans and reports are considered by the Corporate Governance Committee, as is its annual report and assurance statement on the effectiveness of internal controls.

Internal audit has the right of access to such information and records as necessary for the effective performance of its work and staff are required to co-operate in a timely manner in response to a request for assistance or provision of information.

External audit

The annual accounts of the Assembly Commission are audited by the Auditor General for Wales (AGW) under Section 137 of the 2006 Act. The AGW is also empowered to undertake value for money examinations into the Commission's use of resources (Section 139). The accounts and any reports by the AGW are laid before the Assembly and published, and the PAO may be required to give evidence to the Assembly's Audit Committee in respect of them.

The Wales Audit Office (the staff of the AGW) will undertake any external audit work on behalf of the AGW. They have wide ranging statutory access to information and documents that they require in the course of their work (paragraph 17 of schedule 8 to the 2006 Act) and staff are required to co-operate in a timely manner in response to a request for assistance or provision of information.

Corporate strategy and budget

To plan for the delivery and development of support to the Assembly, the Commission prepares a corporate plan. This informs the revenue and capital funding requirements for inclusion in the annual budget that is submitted to the Assembly for approval.

The Finance Manager is responsible for producing monthly management reports setting out performance against that budget for consideration by senior management and the Commission.

The Commission may only use resources, apply income and draw cash from the Welsh Consolidated Fund on the basis of a budget motion of the Assembly. The use of resources and cash that exceed the ambit or amounts in approved budget motions will be deemed irregular by the Auditor General for Wales and may result in the PAO being asked to explain the circumstances to the Assembly's Audit Committee.

Accounting

The Commission is required to produce its annual accounts in a form directed by the Treasury. That direction requires compliance with the Financial Reporting Manual. The Commission is also required to maintain proper accounting records to enable accurate complete and timely preparation of its accounts and to provide comparable and consistent information for the management of its business (management accounts). The Finance Manager has overall responsibility for the maintenance of such records.

Accounting records should be retained in accordance with the Commission's policy on records management.

Internal controls

The Commission's system of internal control is designed to provide:

- efficient and effective operational procedures;
- timely and reliable reporting of financial information;
- compliance with laws and regulations;
- proper use of public funds;
- economic, efficient and effective use of resources and safeguarding of assets; and
- effective identification and management of risks, and sound corporate governance.

The system of internal control is subject to regular review by the internal auditors who conclude on its effectiveness in their annual report.

Fraud

The Commission will not tolerate fraud of any kind including employee fraud. Any indication of fraud by Commission employees will be investigated and may be reported to the police. Disciplinary action will also be taken which could lead to dismissal.

All staff are responsible for reporting to their own line management (or to the Finance Manager or Internal Audit) any suspected fraud by employees, contractors or suppliers.

Banking arrangements

No bank account may be opened unless specifically approved by the Finance Manager. The operation of any bank accounts maintained must be in accordance with their mandates and for the purposes approved by the Finance Manager.

Cash floats

Cash floats may only be held with the approval of and in accordance with instructions issued by the Finance Manager. The holding of such floats is to be maintained at as low a level as appropriate to their effective management.

Asset management and inventories

Staff are responsible for ensuring that the Commission's assets are protected and maintained in an appropriate manner. Fixed assets and other assets of value are to be recorded on inventories in the manner prescribed in the financial procedures. The Finance Manager is responsible for making periodic arrangements to verify the existence and condition of the assets recorded in the inventories.

Assets that are surplus to requirements must be disposed by the most appropriate method with a view to maximising the disposal proceeds.

Procurement of goods and services

All purchases of goods and services must be covered by an appropriate contract, purchase order or purchasing credit card arrangement. The procedures to be followed and the authorisation levels are set out in the Procurement Guidelines and Purchasing Credit Car procedure. These are designed to secure value for money and ensure compliance with laws and regulations including the EU procurement rules.

Goods and services procured must be used only for the purposes of the Assembly Commission – use for personal, non-business benefit is strictly forbidden.

Income

Any sums due must be notified promptly to the Finance Manager who is responsible for ensuring prompt collection.

In the event of non-recovery, the steps laid down in the financial procedures should be followed. Write-off action should only be taken after every effort has been made to secure collection. Write-offs can only be approved by the PAO.

Losses and special payments

The Finance Manger is responsible for maintaining a register of losses and special payments.

Any losses whether due to losses of cash or inventory items, non-recovery of amounts due, or fruitless payments, must be notified to the Finance Manager in writing setting out the circumstances under which the loss occurred.

Special payments (e.g. ex gratia payments) can only be authorised by the PAO. If such action is contemplated prior approval should be sought before making any offer or commitment. Requests for approval should be in writing to the Finance Director setting out the circumstances of the case.

Gifts and Hospitality

Under the Prevention of Corruption Act 1916, *"it is an offence for a member of staff corruptly to accept any gift or consideration as an inducement or reward for doing, or not doing anything in his/her official capacity, or showing favour or disfavour to any person in his/her official capacity."* Under the Act, it is assumed that any gift or consideration made to an employee of a public body has been given or received corruptly unless the contrary can be proved.

- Gifts to Assembly Members are covered by Standing Order 31 and its Annex.

- The procedures for dealing with gifts offered to individual staff members are covered by the National Assembly for Wales Terms and Conditions of Service Code, available on the HR intranet pages. Any member of staff or his/her immediate family should not *offer* gifts, hospitality and entertainment unless it is normal in the circumstances and the value is modest. All such gifts, hospitality and entertainment should be authorised in advance by a senior manager and recorded in the gifts and hospitality register held by each Directorate.
- Staff who are paid a fee to make speeches, give lectures or provide similar services as part of their official duties must remit the fee to the Assembly Commission but may accept accommodation and meals that are reasonably provided in connection with a related event.
- Gifts offered to a 'Group' within the Assembly, such as a Committee, are covered by HR guidance titled "The Receipt of Gifts by Committees and Other Groups Within the Assembly Parliamentary Service", available on the HR intranet pages.

Declarations of Interest

A member of staff who has or whose family has a material interest in any financial matter including procurement is required to declare that interest to the Finance Manager.

Annex 6

May 2007

Commission

ICT Security Policy

PURPOSE

1. To seek Commission agreement on the ICT security policy (Code for the Use of Assembly ICT Facilities) for Assembly Members, their support staff and other users of the AMAC/BF domain and to acquaint the Commission with the Government security policy that Commission staff must adhere to.

BACKGROUND

2. Members, their support staff and Commission staff are on the same WAN (Wide Area Network); however, there are two separate domains requiring different security policies. Members' and support staff data is held on the AMAC domain (soon to be BF) whilst Commission data is held on the HF domain. The HF domain is part of the GSi (Government Secure intranet), which provides a secure route for electronic communications between connected GSi organisations (Government Departments) and has strict security policies in place.

3. The AMAC/BF domain was created in 2002 to allow Members and their support staff to be released from GSi; creating a separate, more appropriate, security policy, widening the technological possibilities open to Members whilst ensuring that some restrictions remain in place to protect the integrity and confidentiality of the information on the Members' domain.

ISSUES

4. In February 2005 the House Committee considered an initial security policy document which Members later agreed to adhere to; this is the Code for the Use of Assembly ICT Facilities. In January 2007 the Shadow Commission reviewed this document and was advised that some minor amendments would be required to the Code for the Third Assembly; mainly due to recent changes in the technology provided to Members. A draft of the revised Code for the Use of Assembly ICT Facilities is attached at Appendix 1. The Code includes sections of rules that must be adhered to, along with guidance that it is recommended

Members follow. Additions to the Code include items on BlackBerry devices and the storage of image, game and video files.

5. In October 2006 the House Committee took the decision that Commission staff should remain on GSi until such time as the legislature decides upon its long-term ICT strategy. A Code of Connection (CoC), setting out procedures that must be followed by Commission and Welsh Assembly Government staff, is required to allow continued access to the Government GSi network and the WAN, this is attached at Appendix 2; however, some further changes may be required.

6. Commission staff must continue to sign the Government ICT usage rules before access to the network will be granted. Some minor amendments will be required to these rules subject to agreement between Government and the Commission. These rules can be found at Appendix 3.

COMPLIANCE

7. There are no compliance issues.

FINANCIAL IMPLICATIONS

8. There are no financial implications.

RECOMMENDATIONS

9. It is recommended that Commissioners:

- agree that Assembly Members be asked to sign up to the Code for the Use of Assembly ICT Facilities;
- agree that Assembly Members ensure their staff sign up to the Code for the Use of Assembly ICT Facilities;
- agree that Assembly Members and their staff who fail to sign the Code will not have access to ICT facilities;
- note the Code of Connection;
- note the Government ICT usage rules that Commission staff will continue to sign.

Appendix 1

Assembly Members and Support Staff
Code for the Use of Assembly ICT Facilities

1. Introduction

1.1. Since 1st May 2004 the Merlin Alliance has worked in partnership with the Assembly to provide and support the Information and Communications Technology (ICT) operation.

1.2. Following the implementation of the Government of Wales Act 2006 in April 2007 the Legislature separated from the Executive (Welsh Assembly Government) to become a separate legal entity, still called the National Assembly for Wales. The National Assembly Commission (the Commission) is responsible for ensuring that the ICT facilities meet Assembly Members' (AMs) requirements and for monitoring their use. The Commission is supported and advised in this role by its ICT team and the specialists within Merlin. The ICT team of the Commission is also available for information and guidance.

1.3. ICT is provided for Assembly Members and their Support Staff (AMSS) to assist Members in their work as democratically elected members of the Assembly. In common with all other Assembly services, AMs have a duty to ensure that they and their staff use the ICT facilities appropriately. AMs are responsible for the use of all ICT hardware and software by their staff and are advised to include a policy on acceptable use of computer systems in their staff contracts.

1.4. In order to protect the integrity of the computer network and other ICT services and not bring the Assembly into disrepute, AMs have responsibility for ensuring that they and their staff adhere to the *Code for the Use of Assembly ICT Facilities*. Guidance which is not part of the Code is at Annex 1.

1.5. The ICT systems used throughout the Assembly, including the Welsh Assembly Government, are closely integrated but have deliberate areas partitioned for specific use, such as the BF domain (the Members' section). The system is large and complex and inappropriate use by any user can threaten the integrity of the system. It is therefore in everyone's interest that all users understand and adhere to the *Code for the Use of Assembly ICT Facilities*. New AMs and AMSS users are required to confirm that they have read and understood the Code before being given access to the system. Training or advisory sessions can be made available where required.

1.6. Relevant Merlin/Commission staff are required to report to the Head of ICT any instances of misuse of the facilities as set out in the Code.

2. Monitoring

2.1. All communications and stored information sent, received, created or contained within the Assembly's system should be considered as private but may be checked in accordance with the law or for the reasons stated below.

2.2. In consultation with the Presiding Officer, the Commission on behalf of the Assembly, reserves the right to access any communication made or received by an AM or AMSS using the Assembly ICT facilities, including computers and the telecommunication system, without prior notice, for the following purposes:

i. To help maintain compliance with regulatory or self regulatory practices.
ii. To establish facts and protect the interests of the Assembly and individuals.
iii. To prevent unauthorised use of the Assembly's telecommunication system and corporate ICT system.
iv. To prevent inappropriate/offensive media and viruses from entering the workplace.
v. To forward e-mails to correct destinations.
vi. To assist with the investigation of a crime.
vii. To comply with the Assembly's access to information obligations under the Data Protection Act 1998 and the Freedom of Information Act 2000.

2.3. The Assembly also reserves the right to make and keep copies of all information, (including but not limited to telephone calls, e-mails and data documenting use of the telephone, e-mail and Internet systems) for the purposes set out above.

3. Accessing ICT Systems

3.1. It is a breach of the Code to attempt to log on as another user or access any computer system that you have not been given explicit permission to access.

3.2. You must not allow anyone else, e.g. a visitor or contractor to use your username and password.

3.3. Passwords are 9 characters minimum in length, and should use alphanumeric and special characters and a mix of upper and lower cases.

3.4. You will be asked to supply a new password every 90 days. You can change it more frequently if you wish.

3.5. You must not share your password or any PIN or ask others to divulge theirs, to do so exposes private and/or sensitive information to potential misuse. Allowing unauthorised people to access the system by informing them of passwords also enables them to pose as an AM or an AMSS by sending emails from their email address. In circumstances where it is necessary to permit colleagues to access email inboxes it is possible to enable that to happen at a variety of levels, from read-only to full access, without disclosing passwords or permitting access to other files. This is also true of other parts of the system.

4. Care of ICT equipment

4.1. Ensure workstations on the ICT network are switched off during the night. You will be informed if there is a need to leave them on for automatic software updates;

4.2. You must report immediately any loss or damage of ICT equipment to the Members' Service Desk; provided reasonable steps are taken no claim for a loss will be made against you;

4.3. Do not leave ICT equipment unattended during transit or in a public place;

4.4. Lock ICT equipment in the boot of a car or out of sight; if it is not possible to do this, then equipment should either be hidden or not left unattended.

5. Protection of Information

5.1. You should store data on network drives, e.g. H: and P: so that it can be backed up; laptops will automatically save data onto the network after remote use, you must not attempt to disable this synchronisation setting.

5.2. You must lock workstations when unattended, even if only for short periods of time, to prevent unauthorised access to data and emails. This will reduce the risk of others accessing private or sensitive information or sending unauthorised emails.

5.3. Never divulge information that could compromise system security (e.g. password or login details).

5.4. If you believe someone has accessed your system without appropriate authority you should inform the Members' Service Desk immediately.

5.5. Any observed or suspected security weaknesses or threats (be they physical, procedural or ICT related) to assets, including people, information, systems or services must be reported to the Commission ICT Security Analyst.

6. Removable Media and Devices

6.1. Removable devices, such as USB devices must be obtained through centrally agreed arrangements.

6.2. You must not attach, or attempt to attach any device to the network that has not been approved by the Members' Service Desk. Similarly, you must not connect any Assembly device to any other network or computer without approval.

6.3. Introduction of non-approved devices could affect the performance of the network. Repairs to systems that have been damaged in this way may incur a charge. See Annex 2 for further information on breaches of the code.

7. Mobile Working

7.1. Equipment such as laptops and mobile devices, and the information they contain, are particularly vulnerable to theft. As such you must make all reasonable endeavours to ensure that they are protected at all times:

i. Mobile devices must use all available security protection such as passwords, keypad locking and PIN codes to prevent unauthorised access.
ii. Laptops and mobile devices must be stored in a secure location overnight.

iii. Whenever possible, carry portable equipment as hand luggage.

7.2. Laptops must connect to the corporate network at least once every two weeks to:

i. Allow anti-virus software and the operating system to be updated.
ii. Enable files to be backed up on the network file system.

7.3. Remote access via the Internet must be made through the approved VPN (Virtual Private Network) connection only. You must only use the wireless or remote access set-up as configured by the Members' Service Desk.

8. Working at home

8.1. Equipment provided by the Assembly for use in the home must only be used by AMs and their staff.

8.2. Connection to the corporate network via your home PC is not permitted.

9. E-mail

9.1. All emails that enter/leave the Assembly's network are scanned for viruses, spam and inappropriate images. You should also refer to section 2 Monitoring. It is not easy to define what constitutes an inappropriate image but as a general rule it is not acceptable to email any picture that includes full or partial nudity, i.e. emailing any image that could cause offence to another person. This includes images that are classed as 'soft porn', e.g. page 3 pin-up type pictures. Images that are seen by some as humorous can cause offence to others.

9.2. You must not knowingly access or send e-mails containing inappropriate material, the contents of which may bring the Assembly into disrepute.

9.3. You must not automatically forward emails from your email account to another account. You could inadvertently set up an email loop that crashes the email system. For the same reasons, when setting your out of office message you must use the Out of Office Assistant (Tools menu, Out of Office Assistant). You must not create an out of office rule that automatically responds to every email that you are sent.

9.4. **The potential legal liability.** Users may, by use or misuse of e-mail be exposed to potential legal liabilities. For example you may breach discrimination law as embodied in the Sex Discrimination Acts 1975 and 1986, Race Relations Act 1976 and Disability Discrimination Act 1995. These laws apply to you as individuals and also as an employer. If you have any queries about the content of an e-mail (received or to be sent) you should consult either the Members' Service Desk. The Assembly's Equality Policy also applies to all e-mail content. If in doubt, do not send the e-mail.

9.5. E-mail carries legal risks for the user and the Assembly (called "vicarious liability") from the accidental or deliberate infringement of laws including but not limited to:

i. Defamation

ii. Obscene and blasphemous material
iii. Protection of Children Act 1978
iv. Discrimination/harassment
v. Unwanted contract formation
vi. Copyright, designs and patents
vii. Data protection and privacy, Human Rights
viii. Computer crime e.g. Computer Misuse Act , Telecommunications Acts, Regulation of Investigatory Powers
ix. Trademarks

9.6. You must ensure that Internet e-mail accounts, e.g. hotmail accounts are not accessed from the internal computer network; emails and documents from these types of accounts can cause virus infected files to bypass the usual protection system and therefore should never be opened.

10. Internet

10.1. All internet use is carried out at your own risk. The Assembly accepts no liability for any loss or damage suffered by any user arising from personal use of the Internet.

10.2. Note that if a site is deemed unsuitable or inappropriate for users, access to it will be blocked.

10.3. Downloading software and data from the Internet may affect or damage the performance of PCs and laptops, repairs to systems that have been damaged in this way may not be included within the stipulated Merlin contract terms and may incur a charge which may be passed on to the Member. See Annex 2 for further information on breaches of the code.

10.4. You must contact the Members' Service Desk to gain access to software that is required to be downloaded from the Internet.

10.5. Certain web-sites offer to download the latest versions or upgrades to existing software such as "Shockwave" as soon as you visit them. You must always indicate "No" to such offers.

11. Viruses

11.1. Viruses, Trojans and Worms can cause considerable damage to the Assembly's systems and its ability to access its information. Common sources for viruses are:

i. Email attachments.
ii. External networks.
iii. The Internet.
iv. File sharing with external PCs using floppy disk, CD ROM or other removable media.

11.2. You must ensure that all floppy and CD disks received are scanned, regardless of their source, before files are opened on PCs, laptops or the network.

11.3. To avoid inadvertently opening an email with a virus attached, do not use the facility that automatically opens the next mail in the inbox.

11.4. In the event of a virus outbreak, users must follow the instructions given by the ICT Security Analyst or Members' Service Desk to protect the Assembly's systems.

11.5. All new systems that are intended to send and receive information electronically from an external source must be cleared with the Members' Service Desk.

11.6. You must not attempt to disable anti virus software.

11.7. The deliberate introduction of a damaging virus is a criminal offence under the Computer Misuse Act 1990.

12. Personal Use of Official ICT Systems

12.1. All ICT equipment and mobile devices are provided for the purpose of undertaking Assembly business. Members and their staff must not use hardware or software paid for by the Assembly for election campaigning purposes, software provided to up-date Members' personal web sites remains the property of the Assembly, Members may use hardware or software paid for by the Assembly for electoral or party political purposes closely connected with Assembly business and assuming there are no additional costs to the Assembly;

12.2. No personal files should be stored on public network drives. Personal data should be stored on your H: drive.

12.3. Music, video, games, movie clips, films, animations and image files may only be stored on the network if they are connected with Assembly business. This includes shared and personal network drives (P: and H: drives).

i. You are responsible for ensuring that they do not infringe copyright. You must not store any of these file types on the network (including the hard disk of your computer) if the files are of a personal nature and are not for Assembly business use.

ii. If you receive one of these file types (e.g. in an email from a friend) you must delete it immediately from the system. You must not store it on the network or forward it on to anyone else, including your own personal email address. If you have a personal email address (e.g. at home) you should give this to your friends/family for personal correspondence rather than your Assembly email address.

iii. You must not under any circumstance rename a file to hide its contents e.g. renaming a .jpg image file to .xls so that it appears to be a spreadsheet. Similarly, you must not embed any of the above file types in another format, e.g. pasting image files in to a Word document so that they do not register as images on the system.

12.4. You must ensure all data, including that stored on personal drives and removable media, complies with legal requirements such as Data Protection.

13. Software

13.1. You must not load or attempt to load software that has not been impact tested by Merlin and authorised by the Commission; advice should be sought via the Members' Service Desk, ideally before the software is purchased. See section 10 for specific information on downloading software from the Internet.

13.2. Copying software that has been bought for someone else on the network is a potential infringement of license and copyright.

13.3. You must not use software paid for by the Assembly for election campaigning purposes, software provided to up-date Members' personal web sites remains the property of the Assembly, Members may use software paid for by the Assembly for electoral or party political purposes closely connected with Assembly business and assuming there are no additional costs to the Assembly. See section 10, personal use of ICT.

13.4. You should be aware that software provided to update Members' personal web sites remains the property of the Assembly and may be withdrawn if misused.

13.5. Unauthorised software can be identified through routine checks on the network. In an event unauthorised software is identified the Commission Head of ICT will be informed

14. Breaches of the Code

14.1. Failure to comply with sections 2 to 13 of the Code constitutes misuse and will be deemed to be breaches of the Code and therefore subject to the measures detailed in the section entitled Breaches of the Code at the end of this document, see Annex 2.

Annex 1

Guidance - It is recommended that AMs and AMSS adhere to the following.

1. Accessing ICT Systems

1.1. You should not disclose passwords to anyone; if Members have to inform the Members' Service Desk, so that the PC or account can be reconfigured, then the password should be changed immediately afterwards.

1.2. You should not use easily-guessed words as passwords (e.g. "password") nor write the password down. If you believe your password has become known to someone else you must immediately change it.

1.3. You should not allow any passwords to be entered automatically by "auto-complete" facilities or macros, the information will be stored on the desktop allowing other users to possibly access confidential information.

1.4. If you have forgotten your password call the Members' Service Desk.

2. Care of ICT equipment

2.1. You should take all reasonable endeavours to ensure portable ICT equipment is protected at all times; provided reasonable steps are taken no claim for a loss will be made;

3. Protection of Information

3.1. The C: drive should not be used for storing information. Information on the C: drive is not backed up and can be accessed by other desktop users. Transfer the data created on the laptop C: drive to the network at the earliest opportunity and then delete it from the laptop.

3.2. In line with records management procedures for protecting hard copy restricted information, if you need to hold sensitive or restricted information on floppy disk, CD ROM (or other removable media) then they should be stored securely, under lock and key, when not in use.

3.3. AMs and AMSS should be aware of the advice that has been issued by the Commission concerning the application of the Data Protection Act to information which Members and their support staff store on computers.

4. Removable Media and Devices

4.1. Data held on removable media storage devices such as CD, floppy disk and USB memory stick is vulnerable to loss. Such devices are also a ready source of virus transmission.

4.2. Care must be taken to ensure that data transferred onto the Assembly systems via removable media is appropriate. Contact the Members' Service Desk if you are unsure.

5. Mobile Working

5.1. When working remotely, you are responsible for making backups of your work. Store the backup securely in a separate location to the laptop.

6. E-mail

6.1. Inappropriate or suspicious emails (such as unsolicited emails requesting personal information) should be forwarded to the Commission ICT Security Analyst.

6.2. Sender information in an email can be forged or generated by a computer virus; any suspicions that emails have originated from an unauthorised source should be checked by seeking oral confirmation from the sender that they were the sender of the email.

6.3. Contact the Members' Service Desk before opening unexpected attachments, particularly if the sender's name is not recognised; e-mail messages, sent outside the Assembly, might not be secure, therefore particular care should be taken with regard to content. If confidential material needs to be sent outside the Assembly, consideration should be given to the security of the recipient's system.

6.4. Treat e-mails in the same way as letters written on Assembly letterhead paper; e-mail messages can be disclosed in court proceedings.

6.5. You should avoid using HTML format stationery or digitally signed emails. Using these can increase the email size, which may slow delivery times; the recipient may also use the signature for malicious purposes.

7. Internet

7.1. Merlin carry out regular Internet usage surveys across the network, the purpose of which is not intended to identify individual users, but to ensure that there is sufficient capacity to link Internet usage to particular machines and/or users.

8. Viruses

8.1. You should contact the Members' Service Desk before opening unexpected attachments, which may contain a virus, particularly if the sender's name is not recognised.

8.2. A large number of hoaxes are in circulation and overreacting to them can cause as much of a nuisance as some real viruses. **You should not circulate a virus warning via e-mail or otherwise.** If you are concerned about an item you have received contact the ICT Security Analyst.

8.3. You should inform the Members' Service Desk immediately if notified by an outside body that a computer virus may have been sent or received.

Annex 2

Breaches of the Code

1. Breaches of the Code, that constitute misuse, including those identified by Merlin engineers during the course of their normal activities, will be brought to the attention of the Presiding Officer and where the breach is by a Members' support staff, to the Member concerned. In the case of other breaches of the Code, the Commission Head of ICT may approach the Member and attempt to resolve the breach without the need for further consultation.

2. Where an investigation is thought necessary, authority to proceed will be sought from the Presiding Officer. Any such investigation will be carried out by a senior member of the Commission.

3. The Presiding Officer will be kept fully informed. Such investigations can involve seeking reports from specialist software used by Merlin. This software may detail what has been accessed, received, sent or stored by individuals or systems. In such specific cases the Merlin security specialist may themselves access a user's mailbox, C: drive, H: drive or P: drive.

4. Access to a system will only be made where there is a reasonable suspicion that there has been a breach of the Code and then only to the extent necessary to determine whether such a breach has or has not occurred. Once an investigation has been completed the Commission Head of ICT will ensure that any access established as part of the investigation is removed.

5. If during the investigation inappropriate software is found to be residing on the computer system of an AM or their AMSS the Presiding Officer will be informed.

6. Evidence will be disclosed to the police if there is reasonable suspicion of criminal activity.

7. Where it has been considered that misuse has occurred and there is a breach of the Code, this will be reported to the Presiding Officer. The Presiding Officer may decide to refer the matter to the Standards Committee. [1] Facilities and services may be withdrawn if the actions of an AM or an AMSS threaten the integrity of the system or are likely to bring the Assembly into disrepute.

8. A user will be held responsible for claims made against the Assembly arising out of legal action brought as a result of the user's use of the Internet.

9. Loss of equipment through negligence or ignoring advice contained in this Code may result in the designated user or holder of the equipment being liable to pay for the restoration of the equipment.

[1] This is subject to agreement of the Standards Committee and any required change to Standing Orders.

Appendix 2

WELSH ASSEMBLY GOVERNMENT
CODE OF CONNECTION FOR ACCESS TO THE GSI NETWORK

I will ensure that my organisation complies with all relevant legal requirements, including those of the Data Protection Act 1998, Freedom of Information Act 2000, Police and Criminal Evidence Act 1984, Computer Misuse Act 1990 and Regulation of Investigatory Powers Act 2000;

I confirm that my organisation will inform the Welsh Assembly Government (WAG), via the Merlin Service Desk immediately a member of staff leaves my organisation or no longer requires access to the WAG network;

I confirm that all staff within my organisation who have access to WAG's ICT system will sign WAG's ICT Usage Rules (and other related policies as appropriate e.g. the BlackBerry usage policy) before having access to the system;

I confirm that my organisation will take disciplinary action consistent with that used by WAG against staff who have breached WAG's ICT Usage Rules.

I understand that an IT security investigation in to potential misuse of the system by staff from my organisation will be conducted by the WAG Information Security Branch who will liaise with my organisation's Human Resources Department;

I confirm that only equipment supplied to access the WAG network will be used to connect to the WAG network from my organisation and that such equipment will not be used to connect to any other network (note: this does not include connectivity that is facilitated via the WAG internet gateway e.g. House of Commons access, CODA or Snowdrop);

I acknowledge that all communications and stored information sent, received, created or contained by my staff within the WAG system should be considered as private but may be checked in accordance with the law or the 'Monitoring' section of the ICT Usage Rules;

I understand that if requested by lawful authorities, as custodian of my organisation's records, WAG may be obliged to release records relating to my organisation in compliance with the 'Rules on Disclosure - Civil Procedure Rules, 1998, Part 3 - 40th amendment';

I will ensure that all staff from my organisation who need access to the WAG network will be vetted to Basic Check level prior to requesting WAG to permit access;

I understand that staff from my organisation will not have any access to any GSI resource that is not directly controlled by WAG i.e. onward access to other GSI resources will not be permitted (and vice versa);

I understand that staff from my organisation will not have any access to priced online subscription services where paid subscriptions only cover WAG staff and have not been funded by my organisation (and vice versa);

I understand that a limited number of named Finance/Fees Office staff will retain access to the WAG Finance System during April 2007 to facilitate the orderly completion of year-end related processes;

I understand that access by my HR staff to the WAG Snowdrop system will be withdrawn as soon as my own organisation's Snowdrop implementation is fully established;

I will nominate a contact to liaise with the WAG Information Security Team. At the request of the WAG Information Security team, my nominated contact will be responsible for disseminating any IT security related messages within my organisation to all staff who have access to the WAG network.

I understand that staff from my organisation will not have any access to the WAG intranet and vice versa.

Name:

Job Title:

Date:

Signature:

For and behalf of: (connecting organisation)

Appendix 3

INFORMATION SECURITY

ICT USAGE RULES
(FORMERLY KNOWN AS IT SECURITY RULES)

Owner: Michael Harrington, Chief Information Security Officer
Issue Number: 3.02
Date: 9 March 2007
Next Review Date: 9 March 2008

WHO IS THIS POLICY FOR?
All users of the corporate ICT network and official phones including permanent staff, casuals, temporary employees, temporary workers, contractors and secondees.

WHAT IS THIS POLICY ABOUT?
This policy sets out the rules regarding the proper use of the corporate ICT network and all official telephones within the National Assembly for Wales. Failure to follow these rules may result in disciplinary action and possible dismissal.

Contacts: Kath Jenkins, Head of Information Security, 029 2082 6035

Policy Owner: Michael Harrington, Chief Information Security Officer

Publication: this policy is located on the intranet at http://assembly/security

Related Policies:
Information Security Policy – http://assembly/infosecurity

Release Notes
9 March 2007 – additional frequently asked questions added and changed references from UNCLASSIFIED to PROTECT.

22 February 2007 – section 15.6 (Out of Office Messages) added, section 4 (Misconduct) amended to include an example of disregarding standards of storage, section 17.4 (Personal Use of the Network) amended, new Questions and Answers added.

29 January 2007 – Welsh Language image permitted on emails

18 January 2007 – 'Next Review Date' added

20 July 2006 - paragraph 9.4 added to clarify the Classified Information section

April 2006 - This policy has been developed as part of a working group that was formed by the ASPB Merger ICT Shadow Management team.

CONTENTS

1.0 Introduction

1.1 The National Assembly for Wales relies on a variety of database applications and Information Communication Technology (ICT) to support business activities. Proper use of ICT can lead to significant business advantage and these rules are designed to ensure that the ICT network and equipment are used in a way that is both efficient and secure. Improper use may put the Assembly at a disadvantage and expose it to major business risks.

1.2 This document sets out the rules regarding the proper use by ALL staff (e.g. permanent, casual, temporary employees, contractors, temporary workers, secondees) who make use of the corporate ICT network and telephones within the National Assembly for Wales.

1.3 Other networks (e.g. Techniums) exist within the Assembly and different usage rules may apply to the management and use of these networks. If in doubt, this set of usage rules apply and take precedence.

1.4 The Assembly's corporate ICT network and its telephones have been provided for business purposes but some limited personal use is allowed. The conditions on which personal use is allowed are set out in these rules. All users are required to behave in a responsible manner when using the ICT systems and telephones. The rules apply equally to consultants and contractors who are granted access to the Assembly's corporate ICT networks and their contracts with the Assembly must reflect this requirement.

1.5 Staff should also be aware of the Assembly Terms and Conditions of Service Code which deals with conduct matters.

1.6 These rules may be up dated from time to time and will be reviewed annually.

1.7 Failure to follow these rules may result in disciplinary action and possible dismissal.

1.8 Welsh Assembly Government staff should also be aware of the Welsh Assembly Government Security Rules – http://assembly/infosecurity/contents/wagsecurity.htm

1.9 APS Staff should refer to the APS Security Policy - http://assembly/presidingoffic/facilities/content/security/security.htm

2.0 Monitoring

2.1 All communications and stored information sent, received, created or contained within the Assembly's systems are the property of the Assembly and accordingly should not be considered as private and may be checked in accordance with the law.

2.2 The Assembly reserves the right to bypass any password or other security setting you make.

2.3 The Assembly reserves the right to listen to, or have access to read, any communication made or received by an employee using its computers or telephone system without notice for the following purposes:

i. For quality control and staff training purposes.
ii. To help maintain compliance with regulatory or self regulatory practices.
iii. To establish facts and protect the interests of the Assembly and individuals.
iv. To prevent unauthorised use of the Assembly's telecommunication system and corporate ICT system.
v. To prevent inappropriate/offensive media from entering the workplace.
vi. To assist with any investigation by lawfully authorised investigating authorities (eg. Police).
vii. To comply with the Assembly's access to information obligations under the Data Protection Act 1998 and the Freedom of Information Act 2000.

2.4 The Assembly also reserves the right to make and keep copies of all information, (including but not limited to telephone calls, e-mails and data documenting use of the telephone, e-mail and Internet systems) for the purposes set out above, and if it sees fit, to use the information in disciplinary proceedings against employees.

3.0 Breaches to These Rules

3.1 When potential breaches of these rules come to the attention of management, Human Resources will instruct the IT Security Officer to investigate. It is for Human Resources to consider whether disciplinary action in accordance with the Assembly's disciplinary procedures is appropriate.

3.2 Access to the user's systems for the purpose of investigating breaches of these rules, will only be made where there is a reasonable suspicion that such a breach exists. Access will only be made to the extent necessary to confirm that such a breach has or has not occurred, and to establish the details of the breach. The user will be informed that such access has taken place and the reasons for it at an appropriate time. Once an investigation has been completed, if appropriate, the investigating officers will destroy any copies they may have made.

3.3 The Assembly will co-operate fully with the police or government officials of any appropriate level in any investigation relating to unlawful activities conducted using Assembly equipment and systems. If the investigation proves that material has been accessed that is pornographic, advocates illegal acts or advocates violence or discrimination towards other people, this will be considered to be gross misconduct and appropriate disciplinary procedures will be followed, possibly resulting in summary dismissal. In all cases of illegal acts, the police will

be notified. Evidence may be disclosed to the police where there is reasonable suspicion of criminal activity.

3.4 Breaches of these Rules can result in charges of misconduct and gross misconduct. The result of such disciplinary charges being proved can vary from an informal/formal warning to dismissal.

3.5 The IT Security Officer (Kathryn Jenkins, Information Security, 029 2082 6035 or Sian Blake, Information Security, 029 2082 6760) must be informed immediately an IT security breach is suspected or detected. Staff should also speak to their line manager or HR(P) or they may under the Whistleblowing policy inform one of the officers designated there. All such queries will be dealt with confidentially.

4.0 Possible Offences

Misconduct

4.1 The following list of activities, which is not exhaustive, provides examples of conduct considered to breach acceptable ICT usage. To note: all internet (including email) interaction is potentially public. You must be mindful of the context of any emails and the fact that these could enter the public domain. These would normally lead to disciplinary action such as formal/informal warning for a <u>first and accidental</u> offence:

i. Continued personal use of email or the internet at the expense of the interests of the Assembly.
ii. Introducing a virus or causing disruption to normal ICT service through reckless system use.
iii. Downloading, accessing, emailing or otherwise introducing material that causes offence to colleagues or contravenes the Assembly policies such as Equal Opportunities, Dignity at Work, Harassment.
iv. Divulging your password or demanding a colleague share their password with you.
v. Introducing material which infringes copyright.
vi. Disregarding standards of storage, transmission or disposal of information e.g. storing personal movies, graphics/image files, music, animations or games.
vii. Sending email or other electronic transmission which may bring the Assembly into disrepute.
viii. Unauthorised installation of software - whether downloaded from the internet or introduced from disk, CD or other media.
ix. Sending chain mail, unsolicited "spam" or indiscriminate communication.
x. Canvassing, lobbying or propagation of personal opinions such as political or religious beliefs.
xi. Making false claims or denials regarding the use of Assembly systems.

Gross Misconduct

4.2 These are deliberate activities which constitute a major breach of conduct in the use of ICT, bringing the Assembly into disrepute and/or making any further working relationship or trust between the Assembly and employee impossible. Examples would include:

i. Using Assembly systems to commit fraud or other illegal/criminal activity.
ii. Falsifying records, such as logs, email or other electronic transmission.
iii. Downloading, accessing or otherwise deliberately introducing sexually explicit/obscene media into the Assembly.
iv. Introduction of software intending to cause damage to Assembly systems.
v. Using email or other electronic transmission to communicate deliberately threatening or inciting material.
vi. Hacking (attempting to bypass or subvert system security controls) or otherwise deliberately obtaining unauthorised access to corporate systems or other user accounts.
vii. Theft of equipment, data or other property belonging to the Assembly, including personal property stolen from Assembly buildings.
viii. Logging on as another user or accessing any computer system that you have not been given explicit permission to access.

5.0 User Identification

5.1 Access to ICT systems is allocated via a unique username which is protected by a password.

5.2 To obtain access for a new user refer to the Create New User Account form which can be found on the intranet at http://merlinspoc

5.3 It is an offence to attempt to log on as another user or access any computer system that you have not been given explicit permission to access.

5.4 You must not allow anyone else, e.g. a visitor or contractor to use your username and password.

5.5 You can normally log into the network using any machine, however, you should not simultaneously log onto more than one machine.

5.6 Before terminating your employment, you must ensure that any important information held on your account is stored on the shared network drive, and any personal information must be deleted.

5.7 Similarly, line managers should ensure that this is carried out for staff terminating their employment.

6.0 Passwords and PINs

6.1 Passwords are 9 characters minimum in length, and must also consist of both cases, punctuation marks and at least one number.

6.2 You will be asked to supply a new password every 60 days. You can change it more frequently if you wish.

6.3 You must not share your password or any PIN or ask your colleague to divulge theirs. Doing so is considered a serious disciplinary offence.

6.4 Your password must not be familiar and easy to guess.

6.5 You should not allow any passwords to be entered automatically by “auto-complete” facilities or macros.

6.6 If you believe your password has become known to someone else you must immediately change it.

6.7 If you have forgotten your Password you should follow the instructions on the intranet – http://assembly/security

7.0 Health and Safety

7.1 You must make yourself aware of the Assembly's Health & Safety policy which provides advice on workstation assessment and any issues regarding accessibility.

8.0 Care of ICT Equipment

8.1 You are responsible for taking care of the equipment you are using. Such equipment must be procured and disposed of through central arrangements. Personally allocated equipment such as laptops or mobile phones must not be passed on to colleagues.

8.2 Workstations on the corporate ICT network should normally be switched off during the night. You will be informed if there is a need to leave them on for automatic software updates.

8.3 All data must be stored on the network drives so that it can be backed up. Laptops will automatically save data onto the network after remote use. You must not attempt to disable this synchronisation setting.

8.4 Particular care should be taken regarding floppy disks, CDs, USB memory sticks and other removable media. These items are mechanisms for virus transmission and potential loss of data. Please refer to section 6 Removable Media and Devices.

8.5 If equipment in your charge is lost or damaged you are required to report it immediately to the Service Desk. Please be aware that negligent loss or damage is rechargeable and may be considered misconduct.

8.6 Computers and telephony equipment must only be moved by staff who have been specifically authorised to move such equipment.

8.7 Do not:

i. Eat or drink over a computer.
ii. Trail wires where people might trip over them.
iii. Attempt to open computer equipment casings.

8.8 Any equipment, including removable media that is lost must be reported to the Service Desk.

9.0 **Classified Information**

9.1 The Records Management policy details the procedures for classifying all records, including those held electronically. You should also refer to the Security Policy.

Information Classification	**Procedure for Electronic Transmission or Storage**
PROTECT (previously called UNCLASSIFIED)	May be stored on the corporate network and transmitted by e-mail
RESTRICTED	May be stored on the corporate network. Transmitted by e-mail only if the recipient is on GSi*
CONFIDENTIAL	Seek advice from the Service Desk
SECRET	Seek advice from the Service Desk
TOP SECRET	Seek advice from the Service Desk

*Care must be taken to check the list of recipients so that potentially sensitive or protectively marked information is not accidentally released into the public domain.

Additionally, if you are not sure whether an e-mail recipient is on the GSI, examine their e-mail address to see if it contains ".gsi.gov.uk".

9.2 If you need to transmit or store material that is classified higher than RESTRICTED then you must speak to the Service Desk.

9.3 You should be aware that emailing information to a non-GSI recipient is the electronic equivalent of sending the information on the back of a postcard. If you need to email information that is not classified as RESTRICTED, but nevertheless could be regarded as sensitive, you should seek advice from the Service Desk.

9.4 When sending a RESTRICTED email, you must include 'RESTRICTED' in the subject line and also at the start of the message so that the recipient knows that they need to take care when handling the email content

10.0 **Protection of Information**

10.1 You must lock your screen when unattended, even if you only leave your machine for a matter of minutes (use CTRL-ALT-DELETE to do this).

10.2 When accessing or processing sensitive information you should take all reasonable precautions to ensure that your screen cannot be viewed by others – remember your screen may be more easily overlooked than a sheet of paper on your desk.

10.3 In line with records management procedures for protecting hard copy restricted information, if you need to hold sensitive or restricted information on floppy disk,

CD ROM (or other removable media) then they should be stored securely, under lock and key, when not in use.

10.4 You must comply with the Data Protection Act (s) and any other legal, statutory or contractual obligations that is relevant to the Assembly.

10.5 The C: Drive (where accessible) must not be used for storing information. Information on the C: Drive is not backed up and can be accessed by other desktop users.

10.6 Never divulge information that could compromise system security (e.g. password or login details).

10.7 If you are contacted by telephone you must ensure you are aware of the identity of the caller before discussing Assembly official business. This is particularly important should you be discussing information that is sensitive.

10.8 Calls made on mobile phones are very insecure. Conversations in public places can be overheard and scanning equipment can pick up signals and intercept text messages and calls made.

10.9 Mobiles should not be used to discuss information that is deemed to be restricted. Such calls should be made from more secure land lines.

10.10 If you believe someone has accessed your system without appropriate authority you should inform the Service Desk immediately.

11.0 Sharing Information

11.1 There are many ways to share electronic information - some of which are more efficient and/or secure than others. Please see the Best Practice guidance on this to understand the most appropriate method in the context of how you are working.

12.0 Responsibility for Official Systems and Information

12.1 The Assembly makes use of a variety of different computer Application Systems to support business activities. These range from large corporate systems (e.g. The Finance System) through to spreadsheets managed and used by an individual member of staff.

12.2 Each application must have a System or Data Owner who carries overall responsibility for its integrity and defines the criteria under which the data can be accessed or altered. The level of access to systems may be determined by job responsibilities and a minimum amount of training/competence is required before access can be granted.

12.3 The System Owner is responsible for liaison with the Freedom of Information/Data Protection Officer in order to ensure that the Assembly's legal obligations are met.

12.4 Please refer to the Best Practice guidance on the development of end user applications.

12.5 All staff are personally responsible for making themselves aware of the content of the rules contained in this document, adhering to them and for ensuring that no breaches of information security result from their actions (or inactions).

12.6 Line managers have an additional responsibility to ensure staff are aware of the rules.

12.7 Any observed or suspected security weaknesses or threats (be they physical, procedural or ICT related) to assets, including people, information, systems or services must be reported to the Information Security Officer.

12.8 The Departmental Security Officer in HR (E) may have security matters referred to them, see http://assembly/infosecurity/contents/wagsecurity.htm

12.9 Human Resources are responsible for taking the lead in any disciplinary proceedings arising from a breach of these rules by officials.

13.0 Removable Media and Devices

13.1 Removable devices, such as USB devices must be obtained through centrally agreed arrangements.

13.2 You must not attach, or attempt to attach any device to the corporate network that has not been approved through the Service Desk. Similarly, you must not connect any Assembly device to any other network or computer without approval.

13.3 Introduction of non-approved devices could affect the performance of the network. Repairs to systems that have been damaged in this way may incur a charge and may also be subject to disciplinary action.

13.4 Data held on removable media storage devices such as CD, floppy disk and USB memory stick is vulnerable to loss. Such devices are also a ready source of virus transmission.

13.5 Care must be taken to ensure that data transferred onto the Assembly systems via removable media is appropriate. Contact the Service Desk if you are unsure.

13.6 If a CD, floppy disk or USB memory stick contains a restricted document, then special care must be taken with the entire storage device to ensure that it is not used inside an inappropriate environment.

13.7 The use of infrared and Bluetooth devices is currently not configured or permitted on Assembly equipment.

14.0 Mobile Working

14.1 Equipment such as laptops, PDAs, mobile phones, and the information they contain, is particularly vulnerable to theft.

14.2 If you use portable ICT equipment you must make all reasonable endeavours to ensure that it is protected at all times:

i. PDAs and mobile phones must use all available security protection such as passwords, keypad locking and PIN codes to prevent unauthorised access.

ii. Laptops, PDAs and mobile phones must be stored in a secure location overnight.

iii. Avoid leaving ICT equipment unattended during transit.
iv. Whenever possible, carry portable equipment as hand luggage.
v. If it is necessary to leave equipment in a vehicle, ensure that it is locked away and out of sight.
vi. Avoid creating temptation - be discrete in using and storing ICT equipment.
vii. If stolen, the information contained on ICT equipment can become public. If you are accessing or storing sensitive or restricted information, then precautions must be taken to avoid disclosure - see section 9.0 Classified Information.

14.3 When using ICT equipment in a public place - ensure that it is appropriate to do so. Avoid use in "busy" situations and be careful of being overheard whilst speaking on a mobile phone.

14.4 When working remotely, you are responsible for making backups of your work. Store the backup securely in a separate location to the laptop.

14.5 Laptops should connect to the corporate network at least once every two weeks to:

i. Allow anti-virus software and the operating system to be updated.
ii. Enable files to be backed up on the network file system.

14.6 If your working pattern means that you are unable to connect to the network every two weeks then you must contact the Service Desk in order to agree a procedure to allow updates to be delivered to your laptop.

14.7 Remote access via the internet should be made through the approved connection only. You must not attempt to "reconfigure" wireless or remote access set-up.

14.8 Users accessing the Assembly network remotely should be aware of increased security implications of connecting into the Assembly's secure network from a potential insecure location.

14.9 Be aware that 'sensitive' data displayed on PC's in public places can be viewed by onlookers. Ensure you are discreet and never leave the PC unattended.

14.10 Ensure you have logged off at the end of the session.

14.11 If you have misplaced your Remote Access Key Fob you should inform the Service Desk at once.

15.0 Electronic Mail (Official and Personal)

15.1 The Assembly encourages staff to use e-mail as a method of communication. However, it is an easy tool to misuse and you are encouraged to read the additional good practice guidelines.

15.2 All emails that enter/leave the Assembly's network are scanned for viruses, spam and inappropriate images. You should also refer to section 2.0 **Monitoring**. It is not easy to define what constitutes an inappropriate image but as a general rule, it is not acceptable to email any picture that includes full or partial nudity i.e. emailing any image that could cause offence to somebody else. This includes images that are classed as 'soft porn' e.g. page 3 pin-up type pictures. Images that are seen by some as humorous can cause offence to others.

Practical steps to avoid a situation that may cause you to be in breach of the ICT Usage Rules:

- If friends know your work email address, discourage them from sending you images/emails that are in breach of the ICT Usage Rules. Remind your friends/family that all emails entering the network are scanned for viruses, spam and inappropriate images.
- If you do receive an inappropriate email, simply delete it - do not forward it to anyone else within the National Assembly for Wales or outside the network.
- If in doubt, don't send it! Any email that could cause embarrassment to the National Assembly for Wales or could bring the National Assembly for Wales in to disrepute must not be sent from the email system.
- Do not forward unopened emails to anyone else (including your own personal email account). If you have not opened the email yourself, you do not know whether it contains inappropriate material and so it is not appropriate to send such emails on to others (including your own personal email account).
- Do not use the National Assembly for Wales' systems in a way that could cause offence to others. For example, some jokes that you find funny could cause offence to others.

15.3 It will not always be appropriate to communicate by e-mail and you should always consider whether there is a more suitable method (for example where circumstances dictate a need to preserve confidentiality, discussion of sensitive issues which should be communicated face to face or sharing a large attachment with a group of people).

15.4 **The illusion of "privacy".** Between the originator of an e-mail and its recipient(s) a message may be recorded several times. Copies may be retrieved and read by persons other than the intended recipient. You should not write anything in an e-mail that you would not write on a postcard.

15.5 **Ethical issues.** Due to the lack of privacy it is important that nothing is contained within an e-mail, which could potentially be considered as offensive, whether to the recipient or any other person. Jokes or comments that may seem innocent to one person can cause serious offence to another.

15.6 **The potential legal liability.** Staff may, by use or misuse of e-mail be exposed to potential legal liabilities. For example you may breach discrimination law as embodied in the Sex Discrimination Acts 1975 and 1986, Race Relations Act 1976 and Disability Discrimination Act 1995. These laws apply to you as individuals and also your employer. If you have any queries about the content of an E-mail (received or to be sent) you should consult either your line manager, Human Resources or the Service Desk. The Assembly's Equality Policy also applies to all e-mail content. If in doubt, do not send the e-mail.

15.7 E-mail carries legal risks for the user and the Assembly (called "vicarious liability") from the accidental or deliberate infringement of laws including but not limited to:

- Defamation
- Obscene and blasphemous material
- Protection of Children Act 1978
- Discrimination/harassment

- Unwanted contract formation
- Copyright, designs and patents
- Data protection and privacy, Human Rights
- Computer crime e.g. Computer Misuse Act, Telecommunications Acts, Regulation of Investigatory Powers
- Trademarks

15.8 You must not use an email disclaimer for business email, however a disclaimer must be included for personal emails, the wording of which is:

"Any of the statements or comments made above should be regarded as personal and not necessarily those of the National Assembly for Wales, any constituent part or connected body."

"Dyla'r datganiadau neu'r sylwadau uchod gael eu trin fel rhai personol ac nid o reidrwydd fel datganiadau neu sylwadau gan Gynulliad Cenedlaethol Cymru, unrhyw ran ohono neu unrhyw gorff sy'n gysylltiedig ag ef."

15.9 Inappropriate or suspicious emails (such as unsolicited emails requesting personal information) should be forwarded to the Service Desk.

15.10 Except where prior permission has been obtained from the Service Desk:

i. You must not use HTML format to send E-mails.

ii. You must not use graphics for signatures or salutations at the end of an e-mail. The only exception is the use of the authorised Welsh Language logo to denote that you are a Welsh speaker. (The authorised logo is on the intranet copy of these Rules). You must not modify this logo in any way e.g. to re-size it or to change its colour or appearance.

15.11 If you regularly send large e-mails please consider using software such as WinZip to minimise the size of attachments. Advice is available from the Service desk.

15.12 If you urgently need access to someone's mailbox to track down some business related information then you must complete the intranet query form (http://merlinspoc) stating the business justification for accessing another's personal account. You should be aware that access is not automatically granted and may be refused.

15.13 You must not automatically forward emails from your email account to another account. The main reasons for this are that you could inadvertently send RESTRICTED information out of the network and that you could set up an email loop that crashes the email system. For the same reasons, when setting your Out of Office message you must use the Out of Office Assistant (Tools menu, Out of Office Assistant). You must not create an out of office rule that automatically responds to every email that you are sent. If you are away from the office for an extended period of time, your line manager can periodically ask the Service Desk to reset your message so that people who have previously emailed you are reminded of your absence.

Web Based Email

15.14 You must not use Assembly equipment to logon to any non-Assembly based email system. For example, you must not access an e-mail service provided by your home Internet Service Provider e.g. NTL, AOL. The Assembly is currently investigating changes to its security procedures which may in future include access for staff to web-based e-mail.

15.15 Members of the public or other third parties may choose to correspond via private or web based email accounts e.g. hotmail or yahoo. Whilst you are permitted to receive these emails and to respond as appropriate (refer to section 9.0 concerning Classified Information) using the Assembly based email system you must not access web based email.

Out of Office Messages

15.16 Your out of office message must only be used to provide alternate contact details for business purposes. You must not include personal contact details e.g. mobile phone and personal email addresses in your out of office message for the benefit of others e.g. friends and family who may regularly communicate with you via your business email address.

16.0 Internet

16.1 Internet access is provided for the primary purpose of undertaking the Assembly business. The facility may also be used by staff for personal reasons providing that this does not interfere with the need to get the job done nor embarrass the Assembly or its staff. You will be expected to restrict your personal use to within reasonable limits.

16.2 Personal use of the internet must be restricted to non-working time, e.g. during breaks, lunchtimes and before/after working hours. Persistent breaching of this guidance may result in disciplinary action.

16.3 You may shop over the Internet for non-official items. For official purchasing over the Internet, please see the Procurement Manual.

16.4 All internet use is carried out at your own risk. The Assembly accepts no liability for any loss or damage suffered by any user arising from personal use of the Internet.

16.2 You must not access web sites or chat rooms that are offensive, unsuitable or inappropriate to the workplace. The principles here are the same as those contained within the Dignity at Work policy.

16.3 The Assembly restricts access to certain types of web sites. The fact that a site has not been restricted in this way should not be interpreted as its being approved to view.

16.4 Should you accidentally access an offensive web site or chat room, you should leave the site immediately and notify your line management and the Service Desk of the incident.

16.5 If you require access to a barred site for legitimate business reasons a request must be made to the Service Desk via your head of division.

16.6 You must not download software from the Internet as this can affect or damage the performance of the network. Repairs to systems that have been damaged in this way may incur a charge and may be subject to disciplinary action.

16.7 Should you require access to software from the Internet then you must complete the intranet form at http://merlinspoc to gain authorisation.

16.8 Certain web-sites offer to download the latest versions or upgrades to existing software such as "Shockwave" as soon as you visit them. You must always indicate "No" to such offers.

16.9 You must not put on the Internet any material, which incites, encourages or enables others to gain unauthorised access to the Assembly's computer system.

17.0 Personal Use of Official ICT Systems

17.1 All ICT equipment and mobile devices are provided for the purpose of undertaking the Assembly business.

17.2 However, some personal use is allowed provided it is kept within reasonable limits such that:

i. It does not interfere with official duties.
ii. It will not embarrass the Assembly or its staff.
iii. It does not affect the performance of the ICT equipment.
iv. There is no infringement of copyright or other unlawful activity.
v. It is not associated with any personal profit or business profit making with any external organisation.

17.3 No personal files should be stored on public network drives.

17.4 Music, video, games, movie clips, films, animations and image files may only be stored on the network if they are for business use.

- You are responsible for ensuring that they do not infringe copyright. You must not store any of these file types on the network (including the hard disk of your computer) if the files are of a personal nature and are not for business use.
- If you receive one of these file types (e.g. in an email from a friend) you must delete it immediately from the system. You must not store it on the network or forward it on to anyone else, including your own personal email address. If you have a personal email address (e.g. at home) you should give this to your friends/family for personal correspondence rather than your Assembly business email address.
- You must not under any circumstance rename a file to hide its contents e.g. renaming a .jpg image file to .xls so that it appears to be a spreadsheet. Similarly, you must not embed any of the above file types in another format e.g. pasting image files in to a Word document so that they do not register as images on the system.

17.5 You must ensure all data, including that stored on personal drives and removable media, complies with legal requirements such as Freedom of Information and

Data Protection. Additionally, under such laws, this data may be subject to access.

17.6 Personal use of ICT systems must be restricted to non-working time, e.g. during breaks, lunchtimes and before/after working hours. Breaching this guidance may result in disciplinary action.

18.0 H Drives

18.1 H: Drives are for you to use for personal matters e.g. details of leave, flexitime and appraisals.

18.2 They must not be used to store any information that needs to be shared. This includes documents produced in the drafting process.

18.3 You should organise information on your H: drive in a clear and logical manner. For example, create a folder called 'Flexi' and use it to store all of your flexi sheets.

18.4 As with all areas of the corporate network, the Data Protection Actmay permit an individual to have access to data if the individual can be identified from the data held. See 12.4 for more information.

19.0 Working at Home

19.1 The Assembly has a Home working Policy and this can be found at Section 2.2 of the NAWTCSC.

19.2 If you need to work from home on a regular basis a formal request using Annex A of Section 2.2 should be made through line management.

19.3 If ICT equipment is requested it will usually be a laptop which, where the circumstances justify it, can be fitted with remote access capability allowing secure connection to the network from a variety of locations. Laptops can also be provided on a pool basis for groups or to individuals where the business case justifies it.

19.4 Equipment provided by the Assembly for use in the home must only be used by Assembly staff.

19.5 For security reasons, using your own ICT equipment for Assembly business is not encouraged. If you do need to work from home you should borrow a pool laptop. If you do use your own personal equipment for business purposes then you must comply with all of the following:

i. Your computer must be **secure against virus infection** – you must install:
- Antivirus software (with the latest updates),
- A personal firewall,
- Anti-spyware,
- The latest operating system patches.

ii. You must **not work on RESTRICTED** information.

iii. The information **must be de-personalised** while on your PC e.g. remove any references to people and organisations.

iv. The information **must not be accessed by anyone else** – you must remove the information from your computer immediately, including deleted items in the recycle bin.

19.6 Connection to the corporate network via your home PC is not permitted.

20.0 Viruses

20.1 Viruses, Trojans and Worms can do considerable damage to the Assembly's systems and its ability to access its information. Common sources for viruses are:

i. Email attachments.
ii. External networks.
iii. The internet.
iv. File sharing with external PC's using floppy disk, CD ROM or other removable media.

20.2 If you are notified by an outside body that a computer virus may have entered the Assembly network then you must immediately inform the Service Desk.

20.3 However a large number of hoaxes are in circulation and by overreacting to them can cause as much of a nuisance as some real viruses. **You must not circulate a virus warning via e-mail or otherwise to any other member of staff.**

20.4 If you receive a suspicious email with an attachment you must always refer it unopened to the Service Desk for checking.

20.5 In the event of a virus outbreak, users must follow the instructions given by the IT Security Officer or Service Desk to protect the Assembly's systems. Failure to do so may result in disciplinary action.

20.6 All new systems that are intended to send and receive information electronically from an external source must be cleared with the Service Desk.

20.7 You must not attempt to disable anti virus software.

20.8 The deliberate introduction of a damaging virus is a criminal offence under the Computer Misuse Act 1990.

21.0 Software Protection

21.1 Only software obtained through centrally agreed arrangements is allowed on the Assembly's corporate ICT network.

21.2 Copying software that has been bought for another person on the network is not allowed. This may infringe copyright. Should another copy of the software be required you should contact the Service Desk.

21.3 Requests for the installation of new software (including shareware and freeware) must be made using the intranet form at http://merlinspoc

21.4 Unauthorised software will be removed by SBS and disciplinary proceedings may be taken against the employee concerned.

22.0 Telephones

22.1 All Assembly telephones must be used in a professional manner, appropriate to the business of the Assembly.

22.2 Personal use of telephones must be consistent with **Personal Use of Official ICT Systems**. However, such calls should be kept to a minimum and dealt with as briefly as possible so that the use of the lines for official business is not unduly restricted (see use of Mobile Phones below).

22.3 Refer to the Welsh Language policy on the use of greetings and messages.

Mobile Telephones

22.4 If you have an official mobile phone you may make personal calls and reimburse the Assembly for the cost of those calls. To do this, you must request an itemised invoice from your mobile phone provider and highlight all personal calls on the actual bill. The invoice must be passed to Finance Division who will pay the original invoice in full. In order to reimburse the Assembly, you are required to complete a SL8 form listing the calls and include a cheque in full payment.

22.5 Mobile telephones remain attractive items and can be a target for thieves; therefore they should always be used discreetly.

22.6 All available security devices such as key-pad locking codes and pin-codes must be used to prevent unauthorised use in the event of loss or theft.

22.7 Phones must not be left unattended in jacket pockets, handbags or luggage but should be carried and concealed on the individual. See section 14.0 Mobile Working.

22.8 If you are driving and using a mobile phone, you must adhere the Assembly's Driving for Work policy.

22.9 Employees should be aware that mobile telephones can be disruptive. Personal mobile phones should be turned off or set to "silent" during working hours.

Voice Mail

22.10 A pin number must be set by the user on voicemail and this should follow the policy surrounding passwords where appropriate (see section 6.0 Passwords and PINs).

22.11 If, in an emergency e.g. absence due to illness you require access to another member of staff's Voice Mail you should contact the Service Desk.

23.0 Glossary

Application Systems	A program or set of programs that support a business process. Examples might be - accounts systems, a set of

	spreadsheets, payroll systems or a database manipulated with Microsoft Access.
Bluetooth	A radio standard for short distance communication between electronic devices without using wires. It can be used to connect, for example, computers, mobile phones, ear-pieces, etc.
Downloading	Electronically extracting and saving files from a network or the internet to the computer you are using.
Encrypt	The process of converting data into a coded form to prevent it from being read and understood by an unauthorized party.
GSI	The Government Secure Intranet (GSi) is a private computer network providing secure e-mail and a communications hub for shared government IT systems.
Infrared	This is a standard for short distance communication similar to Bluetooth although perhaps not as mobile.
PDAs	Personal Data Assistants are small devices that are capable of holding a copy of your email, calendar, contact list – such that these can be read and written to whilst on the move.
Remote Access Key Fobs	More accurately termed the “Secure ID Token” – this is a small handheld card that displays a constantly changing number. A user must enter this number as well as their username and password in order to gain remote access.
Removable Media	Refers to data storage devices that can be inserted into a computer in order to “save” files – e.g. diskette, CD, DVD or USB memory stick.
Service Desk	Dial 029 2082 5555 - this is your first port of call for all issues and enquiries surrounding ICT use within the Assembly - they have the responsibility for ICT asset procurement.
Spam	Spam now refers to the practice of bulk e-mailing unsolicited messages.
Techniums	Purpose built offices offering “state of the art” facilities with links to academia or specialist industry, designed to assist fledgling businesses with a potential for high growth.
Trojans	Trojans are virus programs that are hidden within legitimate looking files. They are activated inadvertantly - for example, by opening an infected email attachment or downloading and running a file from the Internet.
USB Devices	USB (Universal Serial Bus) is a standard “plug-in” interface between a computer and add-on devices (such as cameras, scanners, keyboards, printers, etc). With USB, a new device can be added to your computer without having to add an adapter card or even having to turn the computer off.

USB Memory Stick	A small USB device which is used to store information – it can be thought of as a more convenient, higher capacity diskette.
Virus	A computer virus is a small program written to alter the way a computer operates, without the permission or knowledge of the user.
Worms	Worms are virus like programs that replicate themselves from system to system over a computer network. They often require no human interaction to be able to replicate themselves.

24.0 Index

Appendix A: Questions & Answers

Q. **I have some business files which fall in to the category of images, movies, video, films, animation, games or music files. Am I allowed to store them on the network?**
A. *Yes. Business files of these types may be stored on the appropriate P drive. However, you may not store any files of these types if they are personal files and not related to business e.g. family photos, holiday pictures.*

Q. **There are a number of images, sample music files and games on my computer that were either installed with a package or came as a standard part of my computer. Do I need to delete them?**
A. *No. You only need remove images, movies, video, films, animation, games or music files that are not work related if you loaded them on to the PC or network e.g. H drive, P drive, email, Archive Vault.*

Q. **The all staff email that was issued on 22 February 2007 referred to storing personal files on the network. Does this mean that I can save them instead on my C drive?**
A. *No. Section 17.4 of the ICT Usage Rules is clear that you may not store personal files relating to images, movies, video, films, animation, games or music on Assembly equipment, including C drives.*

Q. **Can I put my personal email address on my out of office message?**
A. *No. The Assembly's information must be stored centrally so that it is accessible in the event that it needs to be retrieved e.g. to answer a Freedom of Information request or Subject Access request. If you have been using your personal email account to store correspondence, that information is lost from the corporate repository. It also means that the Assembly is contravening the Public Records Act and potentially the Data Protection Act.*

Q. **It is much easier for me to work at home using my personal email address than to borrow a laptop and access my work email account remotely. Is it ok for me to work this way?**
A. *No. You must not use your personal email address to store or process correspondence on the Assembly's behalf. Section 19 of the ICT Usage Rules explain the circumstance when you can use your own computer to work from home.*

Q. **I am an ex-ASPB user, how do I delete items from my legacy email**
A. *When you delete a message in the legacy folders it is not deleted straight away, it is marked as "to be deleted" and will stay in the inbox (although it will have a line marked through it to show it's ready for deletion). You have to actually go to the edit menu and select "Purge deleted items" to complete the deletion process.*

Q. **My colleague has just had a baby and has sent me some photographs via email, can I forward them on to anyone else?**

A. *No. If you want your colleagues to see the picture, ask them to have a look at it whilst it is on your machine. Once you've looked at it, delete it from your email.*

Q. Can I store a small number of family photos on my computer or the network?
A. No. You *must not store any personal images, movies, video, films, animation, games or music files on the network.*

Q. A number of people log on my computer. If anyone else stores personal files on my computer, will I be blamed if they are found on my machine?
A. *No. The username of the person who saved the image is associated with the file. This is why you must never share your username/password with anyone else because you are accountable for all activity that takes place under your username*.

Q. Can I access my private e-mail over the internet from my work PC?
A. *Not currently, access to web based e-mail accounts, such as Hotmail, is prohibited because of the risk of virus transmission into the corporate network. However, you may send and receive email from a web based account that is accessed by your own PC. The Assembly is looking into web-based e-mail.*

Q. I am working away from the office, can I automatically send my e-mail to another account?
A. *No, it could result in the inadvertent forwarding of confidential information or technical difficulties.*

Q. A member of staff is off sick, how do I get access to their e-mail and H drive?
A. *You must complete the intranet query form (*http://merlinspoc*) stating the business justification for accessing another's personal account. You should be aware that access is not automatically granted and may be refused.*

Q. A member of staff is off sick, how do I reset their out of office message?
A. *You must complete the intranet query form (*http://merlinspoc*) stating why the change is required and the form of words for the message.*

Q. How do I virus check removable media?
A. *Individual files are automatically checked as each is accessed and opened. However, it is good practice to check the complete device. The instructions can be found on the intranet.*

Q. Can I attach a modem to my computer?
A. *No, you must not attach any equipment to the IT infrastructure that has not been centrally approved.*

Q. Can I use the Internet for personal on-line shopping?

A. *Yes, but this must only be done during non-working time. However all such use is carried out at your own risk. The Assembly does not accept responsibility or liability for loss caused as a result of use of the Internet.*

Q. Can I download software from the Internet?
A. *No - all software must be approved and impact tested prior to loading onto the Assembly network. If the software is required for business purposes you must contact the Service Desk.*

Q. I've got a CD Rom with some new software on which I need for business purposes. What should I do with it?
A. *All requests for the installation of new software must be made via the intranet form at (*http://merlinspoc*). All software must be impact tested and approved prior to loading onto the network.*

Q. Can I use e-mail for personal use?
A. *Yes - but you must not send personal e-mails during working time. You must also keep personal e-mails a reasonable length and number. Lengthy conversations via e-mail should not be conducted and no chain e-mails should be circulated. All personal e-mails must also be sent with the personal e-mail disclaimer attached.*

Q. A friend/relative has e-mailed me with a warning about a virus. What should I do?
A. *Forward the e-mail onto the Service Desk.*

Q. I've got a CD/floppy disk with some games on that I want loaded onto my PC. How do I go about loading them?
A. *You must not load them onto your PC - only business software authorised by the Service Desk will be allowed Assembly's IT systems. Games are not authorised software unless there is a business case. Unauthorised software will be removed and disciplinary proceedings may be taken against the employee(s) concerned.*

Q. Can I work at home on my own PC?
A. *This is not recommended as the security and integrity of home PCs cannot be guaranteed. Only unclassified data can be worked on and strict criteria must be followed; the antivirus, anti-spyware, personal firewall and operating system software must be up to date and information must be depersonalised and deleted after use. It is preferable to borrow a pool laptop for occasional use, provision for more regular use can be made via the home working policy which also defines eligibility for an Assembly PC for home use.*

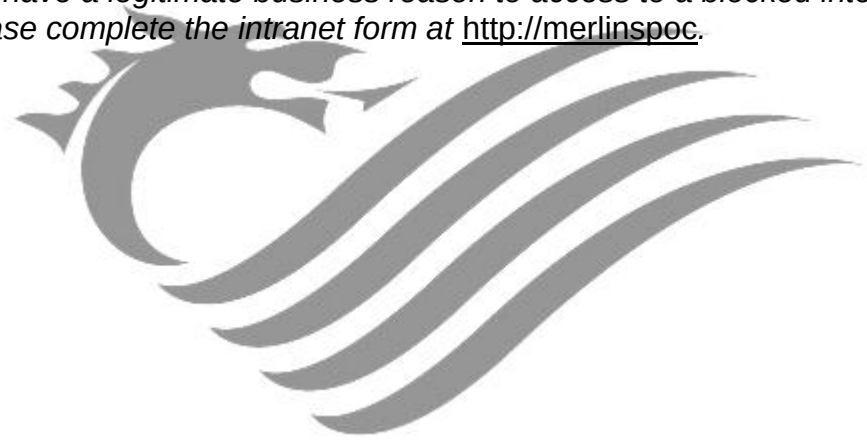
Q. I have just bought a phone that makes use of Infrared and Bluetooth. Can I connect it to my laptop?
A. *No. Only devices procured through central arrangements can be connected to Assembly laptops. At present the use of Bluetooth and Infrared is prohibited.*

Q. I am about to go away on holiday. Can I give my password to a colleague so that they are able to check for important emails while I am absent?
A. *No. Your password is part of your identity and as such must not be divulged to another person (you would not lend someone your driving license to drive your car, or your passport to go on holiday!). You should enable your out of office assistant. You may also give your colleague access to your inbox through their own account, if appropriate.*

Q. Can I access my Email or other Assembly applications from an internet cafe?
A. *No. Access to the network from unapproved machines is not permitted. You may access systems remotely using a pool or issued laptop.*

Q. Can I use my C: drive to store information?
A. *No, in the normal course of events, access to C: drive will be disabled to assist information management requirements. However, under certain cases it may be necessary where a business case justifies the use. (Laptops will utilise the C: drive for remote use and synchronisation. However, this will be hidden from the user and will appear as if they are using their H: drive).*

Q. How do I get access to an internet site that has been blocked.
A. *If you have a legitimate business reason to access to a blocked internet site, please complete the intranet form at* http://merlinspoc.



Annex 7

Cynulliad Cenedlaethol Cymru
National Assembly for Wales
Code of Practice on
Public Access to Information

Contents

1 Code of Practice on Public Access to Information

1.1 Purpose

This Code of Practice sets out:

- the principles guiding our approach to openness;
- the principles under which we will publish information or make it available on request; and
- the circumstances in which we may withhold information.

It also tells you where to seek advice about requesting information and reinforces:

- our commitment to be open about what we do.

1.2 Scope

This Code of Practice sets out the principles by which we will meet our commitments and obligations under:

- section 31 of the *Government of Wales Act 2006* and the
- the *Freedom of Information Act 2000,* the *Data Protection Act 1998* and the *Environmental Information Regulations*, including the rights of access to information and the categories of exempt information specified in those laws; and
- the relevant codes of practice and guidance issued by government departments and by the Information Commissioner.

This Code does not create rights of access to documents. However, when documents are provided, they will be provided in the language of your request if they available in both English and Welsh. If they are only available in one language, they will be provided in that language unless the document consists of fewer than 100 words.

1.3 Principles of Our Approach to Openness

We are committed to the following principles. They are explained in detail in Part 3:

Principle 1 - Maximising openness
Principle 2 - Using clear language
Principle 3 - Maintaining a Publication Scheme
Principle 4 - Publishing on the internet
Principle 5 - Respecting privacy, confidentiality and law
Principle 6 - Prompt and comprehensive responses
Principle 7 - Right of complaint
Principle 8 - Providing information free of charge

1.4 Status

This Code does not override any legal provisions that require or prevent the disclosure of information.

The *Government of Wales Act 2006* formally separates the National Assembly for Wales and the Welsh Assembly Government, and defines the functions of the two bodies. The Act also establishes a body known as the Assembly Commission (the Commission).

The National Assembly for Wales
The National Assembly for Wales (the Assembly) consists of the 60 Assembly Members elected by the people of Wales. The Assembly is responsible for approving most public expenditure in Wales, for scrutinising the actions of the Welsh Assembly Government and for holding it to account. It also has the power to formulate legislation (known as Assembly Measures) in areas for which responsibility has been transferred to it by the UK Parliament.

The Assembly Commission
The Commission consists of the Assembly's Presiding Officer and four other Assembly Members. The Commission must provide to the Assembly, or ensure that the Assembly is provided with, the property, staff and services required for the Assembly's purposes. Information on the Commission's estate, staff and services can be found on the Assembly's website at http://www.cymru.gov.uk

Whilst this Code relates to the Assembly, it will be the Commission which will mainly be responsible for its implementation. In order to avoid confusion for the remainder of the document, we will refer to the Assembly alone, except where there is a need to differentiate between responsibilities. **Where we refer to the Assembly, we do not include information held by Members in their personal or constituency/regional capacities.**

The National Assembly for Wales is listed as a public authority in the Freedom of Information Act 2000.

This Code applies to the recorded information we hold or that is held for us by another person. Except for environmental information, we do not hold information if we hold it on behalf of another person. The code also applies to documents relating to the proceedings of the Assembly, its committees and sub-committees except those from which the public are excluded under the Assembly's Standing Orders.

Contracts with third parties entered into by the Assembly include terms covering the disclosure of information. Information provided by third parties will be considered for disclosure if it is requested.

1.5 Review of this Code

We will review this Code to ensure that we continue to meet legal requirements governing access to information.

2 Requests For Information

2.1 Providing Advice and Assistance

We will, as far as is reasonable and possible, provide advice and assistance on making requests for information. Contact details are given in Part 4.

2.2 Making a Request

You can request information:

• in writing, including by fax or email;
• if you are unable to put your request in writing because of a disability, or for some other reason, you may make a request by telephone or in person:
•requests for environmental information may also be made by telephone or in person.

Requests in writing may be made in Welsh or English. If your request is not in writing, we will write to you to confirm what information you asked for. That letter will be in the language of the conversation in which you made your request.

When requesting information, you must:

• give a name and address to which a reply may be sent;
• give enough detail for us to identify what information you want.
• provide proof of identity when requesting your own personal data. You may be asked to pay a small fee for personal data requests. You may tell us how you would prefer to receive the information. For example:
• a copy of the information;
• by inspecting the information; or,
• a digest or summary of the information.

Whenever reasonable, we will provide information in the format that you prefer. If we cannot do this, we will explain why.

2.3 Which Law Applies?

You do not need to mention which law you think applies to your request for information. We will gather the information you seek and examine it to see which laws apply and then apply them. This may mean that we apply more than one law to your request. You are encouraged to be as precise as possible in your request; if you are not sure what to say in your request, you can ask us for help. You may, if you wish, restrict the information you seek. Doing so may enable us to provide information more quickly as the amount of searching required could be reduced. For example, you could ask us to send you only the personal data you are entitled to under the *Data Protection Act 1998* and we would not send you any personal information, any environmental information or any information covered by the *Freedom of Information Act 2000.*

3 The Principles Explained

Principle 1: Maximising Openness

We will be as open as possible

• We will be as open as possible and only withhold information if it falls into one of the exempt categories or disclosure would breach any other provision of law. Where an exemption is applied we may also apply a public interest test and a substantial harm test, Further details are provided in annex A.
• We will continuously seek opportunities to publish information unless it is exempt under this Code.
• Assembly plenary meetings are held in public. Committee meetings are also held in public except in specific circumstances set out in the Assembly's Standing Orders. Our website has information about these meetings.

Principle 2: Using Clear Language

We will present our business in clear language, in line with our bilingual policies and taking account of different needs

• We will use plain, gender neutral language in our dealings with the public.
• We will aim to produce brief, easy to read documents and will avoid the use of small print.
• We will produce documents in English and Welsh in accordance with the Assembly Welsh Language Scheme.
• We will respect the differing needs of different sectors of the community.

Principle 3: Maintaining a Publication Scheme

We will maintain a Publication Scheme

• The Scheme states our commitment to make information publicly available and sets out:
- the information we undertake to publish as a matter of course;

- how this information will be published;
- whether the information is available free of charge or not.
• The Scheme is published on our website.
• Hard copies of the Scheme will be provided upon request.

Principle 4: Publishing on the Internet

We will publish information on the Internet

• Our website holds information that falls within the categories listed in our Publication Scheme.
• We will provide bilingual websites in accordance with our statutory obligations and our policies on the use of the Welsh and English languages.
• We will publish records and minutes of Assembly proceedings on our website in accordance with the Assembly's Standing Orders. This includes plenary sessions and most committees (except those that the Assembly's Standing Orders allow to meet
in private when that power has been exercised).
• Our website will conform to international and national standards for accessibility.
• Our website will provide search facilities, feedback and contact forms for further enquiries about the availability of information.
• Our website will list significant disclosures of information made in response to requests for information. This will not include personal data disclosed in response to subject access requests under the *Data Protection Act 1998.*

Principle 5: Respecting Privacy, Confidentiality and Law

We will respect personal privacy, the duty of confidence, and all laws governing the release of information

• Before we reply to a request that will involve disclosing information about someone whose interests are likely to be affected by disclosure, we will normally consult them to ensure that any disclosure complies with the law.
• Examples of legislation covered by this principle include the Official Secrets Act 1989, the Data Protection Act 1998, the Human Rights Act 1998, the Environmental Information
Regulations, and the Freedom of Information Act 2000.

Principle 6: Prompt and Comprehensive Responses

We will provide prompt and comprehensive responses to requests for information

• We will send information you request and which is not exempt, promptly and in any case within legal time limits.
• We may send information in several instalments to ensure that you receive as much as possible as early as possible.

• The law sets basic time limits and sets out how, in some circumstances, we may take longer. If we need to take longer, we will write to you explaining why and giving a new deadline.
• If you need our help to make a request we will write to you for confirmation that we have understood your request correctly and so that you have a record of your request.
• Any information we disclose will be in the language in which we hold the information unless the document consists of fewer than 100 words
• If we receive a request in Welsh or English, the covering letter for our reply will be in the same language as the request.
• If we receive a request for information in a language other than English or Welsh the covering letter for our reply will, where practicable, be in that language.
• We do not have to obtain information we do not hold. If we think that another public authority holds some or all of the information, we will consult them and you about transferring your request. We will transfer the request if you agree or, if not, we will provide you with contact details for the other public authority.
• We will always be as open and helpful as possible but will, where appropriate, handle vexatious and repeated requests strictly in line with our legal obligations
• If we refuse to send you information, we will send a refusal within the legal deadline and tell you about our complaints procedure.

Principle 7: Right of Complaint

We will provide a right of complaint where a member of the public is not satisfied with the response received

• We will try to provide the information you request and to avoid providing too much or too little. If this does not satisfy your needs, you are encouraged to contact the person who
responded to your request to discuss ways of providing the information needed. In many cases, it may be possible to meet your needs without using the complaints procedure.
• Our *Code of Practice on Complaints* can be found on our website. Printed copies and advice are available from the Office of the Chief Executive and Clerk.
• In line with our *Code of Practice on Complaints*, any complaint that information which should have been provided has not been, will be investigated. The complaints code explains that you should normally complain first to the person who replied to your request. It also sets out the principles of the Code, one of which is courtesy. This principle states that communication must be based on mutual respect, fairness and trust.
• If, after using our complaints procedures, you are still unhappy with the outcome, you may refer the complaint to the Information Commissioner. Usually, the Commissioner will expect you to have tried our own procedures before investigating your complaint.

Principle 8: Providing Information Free of Charge
We will provide information free of charge where possible

• Our aim is to avoid charging if we can and, if not, to keep any charges as low as possible. We will use our discretion when deciding whether or not to charge, even if we are legally entitled to charge.
• We are allowed to charge for information. We charge for some publications (our Publication Scheme shows which).
• We will only make charges for anything other than publications in exceptional circumstances.
• We may review this principle in the light of experience.
• We will also review this principle in the light of any Fees Regulations made under the *Freedom of Information Act 2000*.

4 Contacts

4.1 Making requests

Access to information requests should be made to

Access to information Advisor
National Assembly for Wales
Cardiff Bay
Cardiff
CF99 1NA
Tel 02920 898889
Email Assembly-accesstoinformation@wales.gsi.gov.uk

4.2 Obtaining Publications

Our Public Information Line can help you find documents published by the National Assembly for Wales. You can contact the Public Information Line on 0845 0105500, text phone 0845 0105678 or by email Assembly.info@wales.gsi.gov.uk

4.3 Booking seats at plenary meetings

You can book seats for meetings held in public by ringing the Public Information line as detailed above, or by emailing assembly.bookings@wales.gsi.gov.uk.

4.4 Complaints

You can get advice about the complaints procedures from:
The Office of the Chief Executive and Clerk
National Assembly for Wales
Cardiff Bay
Cardiff
CF99 1NA
Tel 029 2089 8705

Email aps-complaints@wales.gsi.gov.uk

4.5 Our website

Our website is www.assemblywales.org / www.cynulliadcymru.org.
We publish the agendas, papers and transcripts of plenary and committee meetings and we will also provide information regarding significant disclosures made as a result of access to information requests.

Annex A

Public interest and Substantial Harm Test

The table shows exemption by exemption whether the public interest and substantial harm tests are applied to information falling under the Freedom of Information Act and environmental information regulations exemptions.

- If Annexe A shows that an exemption is qualified, and that we will apply the public interest test and the substantial harm test, we will only rely upon the exemption if disclosing the information would cause or be likely to cause substantial harm to the purpose which the exemption aims to protect. Even if disclosure would cause or be likely to cause such substantial harm, we will not rely upon the exemption unless that harm outweighs the public interest in disclosure of the information;
- If Annexe A shows that an exemption is qualified, and that we will apply only the public interest test, it means that we will only rely upon the exemption if the public interest in withholding the information for the purpose that the exemption aims to protect, outweighs the public interest in disclosing the information;
- If Annexe A shows that an exemption is absolute, and that we will apply the substantial harm test, it means that we will only rely on the exemption if disclosing the information would cause or be likely to cause substantial harm to the purpose which the exemption aims to protect;

If Annexe A shows that an exemption is absolute, and that we will apply neither the public interest test nor the substantial harm test, it means that we will rely on that exemption and not disclose the information.

Derived from the Freedom of Information Act 2000

FoI Act section	Exemption	Absolute or Qualified	Public interest test?	Substantial harm test?
21	Information accessible to applicant by other means	Absolute	No	No
22	Information intended for future publication	Qualified	Yes	Yes
23	Information supplied by, or relating to, bodies dealing with security matters	Absolute	No	No
24	National Security	Qualified	Yes	Yes, except when a certificate has been issued under S24(3)
26	Defence	Qualified	Yes	Yes
27	International relations	Qualified	Yes	Yes
28	Relations within the United Kingdom	Qualified	Yes	Yes
29	The economy	Qualified	Yes	Yes
30	Investigations and proceedings conducted by public authorities	Qualified	Yes	No
31	Law enforcement	Qualified	Yes	Yes
32	Court records, etc.	Absolute	No	Yes
33	Audit functions	Qualified	Yes	Yes
34	Parliamentary privilege	Absolute	No	No
35	Formulation of government policy, etc.	Qualified	Yes	Yes
36	Effective conduct of public affairs	Qualified	Yes	No
37	Communications with Her majesty, etc. and honours	Qualified	Yes	Yes
38	Health and safety	Qualified	Yes	Yes
39	Environmental Information	Qualified	Yes	No
40 (1)	Personal information (about applicant)	Absolute	No	No

FoI Act section	Exemption	Absolute or Qualified	Public interest test?	Substantial harm test?
40 (2)	Personal information about others where the circumstances described in section 2(3)(f)(ii) FoIA are the case	Absolute	No	No
40 (2)	Personal information about others where the circumstances described in section 2(3)(f)(ii) FoI are not the case	Qualified	Yes	No
41	Information provided in confidence	Absolute	No	No
42	Legal professional privilege	Qualified	Yes	Yes
43	Commercial interests	Qualified	Yes	Yes
44	Prohibitions on disclosure	Absolute	No	No

Derived from the Environmental Information Regulations

EIR 2004 regulation	Exception	Public interest test?	Substantial harm test?
12 (4) a	Information not held when request received	Yes	No
12 (4) b	Request is manifestly unreasonable	Yes	No
12 (4) c	Formulated in too general a manner	Yes	No
12 (4) d	Material is still in course of completion, unfinished documents or incomplete data	Yes	Yes
12 (4) e	Internal communications	Yes	Yes
12 (5)	Where disclosure would adversely affect -		
12 (5) a	International relations, defence, national security or public safety	Yes	Yes
12 (5) b	Course of justice, fair trial, criminal or disciplinary inquiry	Yes	Yes
12 (5) c	Intellectual property rights	Yes	Yes
12 (5) d	Confidentiality of proceedings of a public authority where confidentiality is provided by law	Yes	Yes
12 (5) e	Confidentiality of commercial or industrial information where confidentiality is provided by law to protect a legitimate economic interest	Yes	Yes
12 (5) f	Interests of person who provided information where that person: (i) not under legal obligation to have supplied the information (ii) did not supply it in circumstances where the public authority is entitled to disclose the information apart from these regulations (iii) has not consented to disclosure	Yes	Yes
12 (5) g	Protection of the environment to which the information relates	Yes	No

Annex 8

The National Assembly for Wales Commission

Data Protection Policy Statement

The National Assembly for Wales Commission (Assembly Commission) is committed to processing personal information in accordance with the Data Protection Act 1998.

In undertaking its business functions, the Assembly Commission needs to process certain information about Assembly Members, current, past and prospective employees, employees of contractors, customers and other individuals it has dealings with.

The Assembly Commission will ensure that all personal information is processed in accordance with the eight Data Protection Principles detailed within the Act.

The Principles state that personal information shall be:

processed fairly and lawfully;

processed only for specified, lawful and compatible purposes;

adequate, relevant and not excessive;

accurate and up to date;

kept for no longer than necessary;

processed in accordance with the rights of data subjects;

kept secure; and

transferred outside the European Economic Area only if there is adequate protection.

Data Controller

The Assembly Commission is the Data Controller in relation to the processing of personal information.

The Assembly Commission may entrust responsibility for day to day data protection matters to the Chief Executive and Clerk Advisor.

The Access to Information Advisor will manage the notification to the Information Commissioner and providing advice and guidance to Assembly Commission staff. Specific advice will be provided on the processing of personnel data.

All staff are responsible for ensuring that they collect and process personal information in accordance with guidance issued by the Access to Information Advisor.