SECURITY PRACTICE

1. Introduction

1.1 There are, unfortunately, in Local Government many who do not appreciate the need for security other than in its most obvious aspects. The reasons for this are:-

- A lack of awareness of the hazards which exist
- An "it won't happen to me" attitude
- A misplaced trust in others, especially that people are not always who they claim to be
- Over-familiarity with workaday routine matters which tends to create apathy as to what is sensitive or confidential

1.2 Understandably there is often a reaction, consciously or otherwise, against security measures, particularly those which may cause inconvenience. This code will serve as a reminder to all staff of the precautions and safeguards which they will reasonably be expected to take. This code will be given the widest possible circulation. It is anticipated that senior personnel will add weight to the code by example.

1.3 It must be understood that these notes have been prepared and set down for the general guidance of staff and except in special paragraphs – for instance those items under the headings of safes, safe keys and cash in transit where conditions of insurance are specific – the rules are not obligatory but the Council will rely upon the good sense of its officers to pay heed to the notes. Quite obviously local circumstances may differ and a degree of flexibility must exist. In any case a reasonable degree of domestic discipline and good sense must be used.

2. Protection of Information

2.1 The potential harm done by the disclosure of **confidential information** is seldom realised by those responsible for leakages, which are usually due to thoughtlessness, misplaced trust in another person, idle gossip or to gain a feeling of importance.

2.2 An Authority does hold in trust intimate details of matters for which it is responsible affecting both employees and the public generally. All persons have a right to expect that these details are safeguarded.

2.3 The information which requires to be protected comes under three main headings. The itemised matters are examples and are not intended to be exhaustive.

3. Personal Information

Staff records; financial applications; Social Services and Housing matters; and cases relating to alleged breaches of the law and discipline code.

4. Security Measures

Plans showing security features, correspondence on security matters including specifications for security systems and information about security procedures.

5. Development Schemes/Planning Proposals

5.1 The sale and purchase of property and land; relevant Committee matters (particularly Part II agenda); tenders, valuations and contracts pertinent thereto.

5.2 The disclosure to unauthorised persons can be of value for a number of reasons including:-

- Criminal gain
- Commercial gain
- Embarrassment to the Administration; of Councillors (personal or political); and staff. People can be compromised. Leakages can be damaging.

6. Measures to Prevent Disclosure

6.1 Staff who acquire information to which they are not normally entitled must not discuss it. It is important that **access to confidential information is restricted**: even to authorised staff and members of the public.

6.2 An unauthorised person may inadvertently or by design obtain confidential information in several ways.

- by seeing the relevant document or a copy of it
- mistakenly thinking that the receiver of the information (or document) is entitled to receive it
- by accidentally overhearing a sensitive conversation

6.3 To prevent this happening unauthorised personnel coming into possession of confidential information to which they are not entitled must report the facts and reveal their source.

7. Document Control in the Office

7.1 All confidential material must be **locked away** when not required **immediately**. A suitable secure cabinet should be provided for important

documents. **Key control** is an **important** element of security. It is not sufficient to lock up a cabinet or secure area with a key which is freely available.

7.2 Discretion should be exercised in the use of wall charts and display maps exposed for selective information. If required for a specific purpose such as architects' or property development meetings they should not be left on display any longer than necessary and even then under supervision.

7.3 The attitude that precautions are unnecessary is a fallacy. It must be made difficult for an interested party with a sinister motive to discover who the responsible person is or which section is dealing with specific and sensitive matters and thereafter seek out the information required.

7.4 **Pre-authenticated cheques** and **Giro cheques** must be very strictly controlled, dealt with by hand and secured in a locked place.

8. Transmission

Movement of **confidential papers** must be **by hand** whenever possible. Such documents must always be passed under cover, sealed and marked in such a way that tampering is deterred and detectable.

9. Reproduction

9.1 Typing, photocopying etc. of confidential material must be carried out by trusted and substantive staff only.

9.2 Drafts, spoiled copies and carbons, all containing confidential information must be dealt with as **confidential waste** and handled under carefully **controlled** conditions. Shredding machines should be used when provided.

10. Disposal

It is not sufficient just to tear up paper which contains confidential material. It must either be shredded or burnt. This task must be entrusted to established and responsible staff.

11. Information Systems

Information Systems are now an integral part of Local Government administration and provide facilities which are difficult to replace and to which Council have grown accustomed. Loss of or interruption of these facilities would seriously cause disruption.

12. Physical Security

12.1 The areas that accommodate computer equipment, auxiliary machinery and staff, merit special attention to guard against unlawful and unauthorised access. It is important that the main computer suite be given special security attention such as access control; electrical locking; special domestic disciplines and patrols to minimise the risk of criminal damage and theft.

12.2 Distant terminals in other locations also merit special measures. The Head of Information Systems and Technology, tutors at schools and colleges and principal users must have the responsibility for protecting equipment and software against known hazards.

13. Resilience: Integrity: Privacy

The rules and operational conditions which exist in all computer base installations and systems must be observed and the advice of the Head of Information Systems and Technology must be sought to ensure that the system functions efficiently to the benefit of and without prejudice to the Authority.

14. Enquiries

This is essentially a matter of identification.

15. Personal Enquiry

Before any information is disclosed the enquirer's identity must be established beyond doubt. Proof of identity or authority must be demanded.

16. Telephone Enquiry

16.1 Sensitive information must never be given in response to an incoming telephone request. The caller's telephone number must be obtained and enquiries made to establish bona fides. The position on an enquirer's "need to know" or "right to know" must be clarified before information is given to them. It is important that requests for information, however innocuous they might appear to be, should be carefully handled even when the enquirer is know **or** holds senior office **or** appears to have established a "right to know".

16.2 Personnel are reminded that telephone conversations can never be guaranteed as confidential. Listening is possible.

17. Careless Talk

Staff are reminded that discussions in public can be overheard. There is a risk that information discussed may have some value to the person who overhears it. A special risk exists when sensitive and confidential matters are discussed in the presence and hearing of those who should not have access to those matters.

18. Identity Cards

Staff to whom identity cards are issued must keep them safely. **Loss** must be **reported immediately** and cards must be surrendered on termination of appointment.

19. Safes

19.1 It is most important that the quality shall match the risk involved. Users must liaise with the Insurance Manager and the officer responsible for security to ensure that a safe is of suitable quality for its maximum forseeable content. If it is proposed to re-locate or change the use of, or increase the cash-holding content negotiations must be held beforehand with the Insurance Manager and the officer responsible for security.

19.2 Before deciding exactly where an acquired safe is located within a building advice must be obtained from the officer responsible for security in the Authority or the local Police Crime Prevention Officer or both. Attention must be paid to the increased floor load which a safe may impose, particularly on upper floors or floors over basements and cellars. Technical advice will be sought from officers in the Authority responsible for structural engineering.

19.3 **Wall Safes**, generally have limited value as protection for cash and are **not recommended**. The Insurance Section or Internal Audit will determine the loss risk suitability of any safe.

19.4 Advice must be obtained before using or continuing to use **safes of old design,** even for minor risks. Care should be taken to ensure that any safe offers adequate **protection against fire**. This advice can and must be obtained from the officer responsible for security; the Insurance Manager; the Crime Prevention Officer of the Police, or the safe makers.

19.5 The amount of cash retained in even the best quality safes must be the minimum compatible with efficiency. The provision of a safe does not replace normal banking arrangements, as laid down in Finance Instructions or Standing Orders as applying to cash. A safe may enable banking and cash

retention arrangements to be improved upon by providing a secure place in which to hold cash until it can be banked under proper security arrangements.

19.6 All money must **be placed** in the appropriate **safe** as **quickly** as possible after receipt. Where money is being received continuously as in a cash or rent office it must be put in the safe as often as practicable and must not be allowed to build up in the cashier's drawer or till. A system of "milking" the drawer or till must be employed whether or not the cashier is operating behind a properly designed security screen.

19.7 A safe must **not be left open** for any longer than it takes to deposit in or remove anything from it. The practice of leaving a safe open, even for a short period is not allowed. This rule does not apply in respect of a safe used solely for keeping working books overnight.

19.8 When a safe is empty of cash, sensitive or other valuable property and keys, it should be left open and unlocked. Similarly cash registers (tills) when empty and not in use should be left with the drawer open and disconnected from the power supply.

20. Cash in Transit

20.1 Except where a specialist agency or the Authority's own security cash carrying service is employed to take cash to and from a bank or to and from the Council's own cash receiving office the following rules **must** be observed: (The Authority's insurers for the money policy will set specific terms).

20.2 Students or casual staff are not to be used, nor are new employees whose references have not been cleared.

20.3 When nominating employees to deal with cash in transit, take into account their potential vulnerability (e.g. physical frailty or impaired mobility may increase the risk). In cases of doubt, consult the Director of Finance.

20.4 No officer shall be required to carry cash outside a Council establishment in the course of his/her duties, unless the Chief Officer of the Directorate concerned has confirmed with the Director of Finance that all the security limitations imposed by the Council's insurers are being met, and that insured limits are not exceeded.

20.5 The provision of an escort should be considered in all cases and is strongly recommended when larger amounts of cash are being moved. The escort should be the first to leave the cash collection point in order to establish that there is no apparent risk. The escort should walk a few paces behind the person carrying the money to give warning of impending attack and to advise

of possible avoiding action. In cases of doubt as to the suitability of an escort, consult the Director of Finance.

20.6 **Times and routes** of journeys between the two points must be **varied**. Regular or rigid procedures should be avoided. A busy route should be preferred to a quite one if there is a choice. Alternative routes should be investigated as to suitability.

20.7 The use of cash carrying **garments, alarm bags, etc** have some merit but carrying cases and bags fastened to the body are not generally recommended as the risk of injury to the employee is thereby greater.

20.8 It is wrong to pre-arrange departure times for banking journeys when using the services of a hired vehicle, taxi or mini-cab.

20.9 **Night safe banking** at regular times is not recommended. Special care must be taken when using this facility.

20.10 The **decision to resist** or not when thieves demand money by threat of violence rests entirely with the person carrying the cash. Criticism will not be levelled against the employee who hands over money when put in **fear** by some **threat** of or **actual violence**. Generally speaking personnel are advised to hand over the money when they feel a real threat exists.

20.11 All personnel connected with the movement of cash must be especially **vigilant**. Caution and care must be exercised at all times.

21. Safe Keys

21.1 The basic rules for control of safe keys are as follows:-

21.2 Safe keys must be kept **separate** from all other keys and will be unlabelled.

21.3 Safe keys must be kept **on the person** of the authorised holder or user at all times. No such key will be concealed on the premises.

21.4 Safe keys must only be held or handled by responsible and **authorised personnel**.

21.5 Safes must be kept locked at all times and the key removed from the lock. Combination locks will not be left unset or set on manufacturers' standard numbers.

21.6 Spare or **duplicate safe keys** for contingency use must be sealed in a suitable container and controlled by a Senior Officer. Such keys may be kept

in another high quality safe; the strong room; or at the Authority's bank. A record of issue and return will be kept by that Senior Officer.

21.7 Where a safe is fitted with two key locks or two combination locks or one key lock and one combination **two custodians** must be used to open the safe. It is not correct for one person to hold both keys, and both combination numbers or hold the key combination whichever is the case.

21.8 Where a **combination lock** is provided, the number series must be memorised and not, except in exceptional circumstances, committed to writing. Any written record will be sealed and retained as for a duplicate safe key. Combination numbers must be changed periodically but at irregular intervals. The sequence of numbers must be closely guarded.

21.9 **Additional keys** for safes will not be ordered or cut without proper written authority from a Senior Officer after consultation with the Officer responsible for security and/or the Principal Internal Auditor.

21.10 The loss of a safe key or any irregularity coming to notice regarding the combination numbers must be reported at once so that appropriate action may be taken.

21.11 The **number of keys** to a safe must be limited and kept to a workable minimum. Where different authorised personnel need access to the same safe at differing times **and** it is not possible for the safe key to be handed over personally then each such authorised person will need to hold a key.

21.12 Where a safe is provided with a **deposit feature** which is designed to provide an additional dimension to secure cash holding without the requirement of the depositor to hold a key to main body of the safe, sufficient deposit canisters must be available and these canisters only must be used to deposit cash. The depositer will not hold a key to the safe. The depositor will place in the canister a signed record of the sum deposited and will also keep a personal note of that sum.

22. Other Keys

22.1 The principles laid down for the custody of safe keys apply to all other keys. It is essential for personnel to recognise the need for a strong secure place in which to keep keys. Lockable steel key cabinets centrally located within the Administration Section of Departments are preferable. Such cabinets must be securely anchored to a substantial wall and must be used to accommodate all general office and cabinet keys (except safe keys). The keys to any key cabinet must also be controlled and held by responsible personnel. The key cabinet must be kept and locked and the keys removed from the lock. The

legend for the contents of the cabinet must be kept elsewhere than in the cabinet. Keys must not be readily identifiable by name tags affixed. Identification by numbers is preferable.

22.2 It is advisable that a system of controlled issue and return is devised.

22.3 **Lost or misplaced keys** must be brought to the attention of the Section Head so that an investigation and replacement, as necessary, can be arranged.

22.4 **Additional keys,** particularly master suited keys, will only be provided after authorisation in writing signed by a Senior Officer or Section Head.

22.5 Officers responsible for purchasing office supplies and equipment should specify that cabinets designated to hold confidential, valuable or sensitive documents or material be fitted with non-standard locks, the keys to which should be delivered separately and thereafter carefully controlled.

23. Buildings

23.1 Advice as to security measures, locks, alarms, access etc **must be obtained** in the early planning stage of any new building, modification of existing building or reconstruction. To save time and expense subsequently the Director of Technical Services or his delegated representative should consult with the Officer responsible for security and/or the Crime Prevention Officer to ensure that premises being designed or modified are adequately secure and that suitable measures are built into the design.

23.2 The responsibility for **locking up premises** must be laid down specifically and the person(s) detailed to do so must be carefully instructed as to what is required. Locking up procedures are important if losses and serious damage are to be avoided.

23.3 Security defects and inadequacies of premises must be reported immediately and repairs carried out as soon as possible and monitored to completion and satisfaction. Security hazards must be dealt with promptly.

23.4 Where local special procedures are laid down for a particular area, e.g. a cash enclosure of cash office, all personnel must comply; this is on the basis that the rules are properly drawn up in the interests of security and safety of the individual.

23.5 Tools and equipment which could be used to assist in the criminal must be locked away or otherwise controlled.

23.6 Where premises are provided with intruder detection systems (**burglar**

alarms) such systems must be switched on when the premises or that part of the premises are vacated. This duty rests with the delegated office or other employee. The alarm key must be carefully controlled. No additional key may be obtained without written authority from the Departmental Divisional or Section Head who will consult with the officer responsible for security.

24. Plant and Equipment

24.1 Accurate records of issue and return of plant, tools and equipment, particularly hired items, including office machines and teaching aids are essential and must be kept up-to-date.

24.2 Where possible they should be returned to stores at the end of work each day; otherwise they must be secured in a reasonable way. Larger items of mechanical and electrical plant must be immobilised.

24.3 An **inventory**, to include serial and model numbers where applicable, must be kept. This applies to all premises.

24.4 Additional Security of **plant and equipment** can be achieved by careful supervision and by identification measures. Items can often be visibly and **indelibly marked or badged** as to ownership.

25. Vehicles

25.1 All Council owned or Council hired vehicles must be locked whenever left unattended. When finished with for the day they must be parked correctly in the garage or other place provided. Where practicable the ignition keys should be handed in for safe custody, but there will be cases where the driver will need to retain keys owing to the late or early finishing or starting. Keys will not be left in the ignition.

25.2 Local conditions and rules may apply to vehicles kept in multiple accommodation depot buildings and locked yards where it is decided to leave ignition keys in the unlocked vehicles so that the vehicles can more easily be moved in the event of fire or other emergency. Basic depot and premises security will nevertheless apply.

25.3 Property should **not be left overnight** in vehicles which have to be kept in open and insecure parking areas. Batteries and spare wheels must be secured to the vehicle to prevent easy removal.

25.4 Special care must be exercised with vehicles equipped with radio. All radios must be adequately secured to minimise the risk of easy removal.

25.5 Vehicles and accessories and equipment on vehicles must be checked at the commencement and finish of use each day. Any discrepancy or irregularity must be reported forthwith. Special attention should be given to the Vehicle Excise Licence disc and the identity disc on the windscreen issued in respect of the goods vehicle operators' licence.

25.6 Damage to Council vehicles or knowingly caused by Council vehicles must be reported as soon as possible.

26. Parking of Vehicles on Council Premises

26.1 The parking of vehicles on Council property **must be controlled** through the Administration Section of the relevant Directorate. Persistent unauthorised parking may have to be dealt with by appropriate effective measures available to the Authority.

26.2 Unauthorised and irregular parking of employees' vehicles must be discouraged. Legal implications may arise.

26.3 Employees' private vehicles on car parks provided should be locked to avoid loss of and from the vehicle. The Council will not be responsible for loss of or damage to employees' vehicles or their contents.

26.4 **Council property** carried in employees' private vehicles in the category of essential or casual user must be carefully protected: the vehicle locked when unattended and the items put out of sight where possible.

27. Evacuation Instructions

27.1 All personnel will flow the procedures as adopted at the places where they work without fail or hesitation. Evacuation instructions apply to everybody.

27.2 **General:** Leave by nearest exit: do not use lift: do not collect personal effects: assemble as directed: **do not re-enter until told to do so**.

28. Bomb Threats

28.1 As with fire the procedures which apply will be followed without question.

28.2 **General:** Leave by nearest exit: do not use lift: take personal possessions with you: assemble away from buildings, parked vehicles or car parks: **do not re-enter until told to do so**.

29. Prevention

Any employee who is not sure of any parcel, package or object which cannot be identified and which is in or against any building or in or near any motor vehicle should not touch it; should report the fact to someone; and should leave the area and warn others to do the same. Action will be taken by a Senior Officer to notify the property authority for urgent attention.

DO NOT TOUCH TELL SOMEONE

OFFICE SECURITY – GENERAL

- DON'T leave handbags on desks or in view; or wallets in coats
- DON'T leave tea money, money collected for presents or other cash in
- unlocked drawers at any time
- DON'T leave accessible windows open when you are out of the office, especially in warm weather
- DON'T assume the stranger in the building or office is a staff member
- DON'T allow anyone to remove or interfere with office equipment without first confirming authority to do so
- DON'T be pressured or impressed by callers whoever they purport to be. Identity of unknown persons should be checked before acting on requests for assistance or information
- DON'T leave callers alone in any office while enquiries are made
- DON'T assume all staff and colleagues are as honest as you are