DUNDEE CITY COUNCIL

REPORT TO: **Personnel Committee – 17 April 2006**

REPORT ON: **Monitoring System for Internet Violations**

REPORT BY: **Assistant Chief Executive (Management) and the Head of Information Technology**

REPORT NO: **270-2006**

1 PURPOSE OF REPORT

1.1 This report outlines the proposals for implementing systematic monitoring of triggered violations when City Council users are accessing the internet.

2 RECOMMENDATION

2.1 It is recommended that the Committee notes that individual Chief Officers will be responsible for systematic monitoring of internet violations as described below within their departments.

3 FINANCIAL IMPLICATIONS

3.1 Additional costs will be contained within departments' Revenue Budgets

4 LOCAL AGENDA 21 IMPLICATIONS

4.1 None.

5 EQUAL OPPORTUNITIES IMPLICATIONS

5.1 Systematic monitoring of the software alert system will further promote the Council's commitment to strive for equality within the working environment.

6 BACKGROUND

6.1 Employees use internet facilities to access the vast library of information which can assist them to carry out their duties. In addition they have access for personal use during lunch breaks and outwith working hours.

6.2 Each employee who is authorised to have access to the world-wide web, has been issued with personal copies of the Council's Internet Guidelines.

6.3 The guidelines clearly identify examples of unacceptable use of the internet and appropriate action, including disciplinary action, is taken against those who view inappropriate websites or download inappropriate material. The guidelines also state that in event that the internet usage constitutes possible criminal activity, that the information will be passed to the police.

6.4 The guidelines further indicate that the Council's Information Technology Department routinely records and analyses all Internet connections, and that details of sites visited and time spent using the internet can be obtained where violation of these policies is suspected and may be used as a basis for action against such violations.

6.5 As a result of consultation with the police (in respect of best practice in handling situations where is it suspected that the Council's Internet facilities are being abused for criminal activity), a small working group has developed a procedure for systematically monitoring the violations of the internet facilities.

6.6 It is proposed that on a monthly basis, designated senior officers will monitor the categories of violations committed. Support will be given by a designated officer within the Information Technology Department.

6.7 In the event that abuse of the internet facilities constitutes possible criminal activity the Chief Executive, the Assistant Chief Executive (Management) and the Director of the department concerned will be advised of police involvement.

6.8 Employees will be advised of the commencement of systematic monitoring. They will also be reminded of the procedure to be followed if they trigger violations which occur during their normal usage of internet facilities.

6.9 The Chief Executive and the Assistant Chief Executive (Management) will have a corporate overview of the monitoring system. However, each Chief Officer is responsible for the systematic monitoring within their departments.

7 CONSULTATION

7.1 The Chief Executive, all Chief Officers and the Trade Unions have been consulted on the development of this proposal. The Chief Executive, the Depute Chief Executive (Support Services), the Depute Chief Executive (Finance) and the Trade Unions have been consulted on the content of this report.

8 BACKGROUND PAPERS

8.1 None.

J C Petrie
Assistant Chief Executive (Management)

10 April 2006

D White
Head of Information Technology

10 April 2006

Appendix 1

INTERNET VIOLATIONS PROCEDURE – GUIDELINES FOR CHIEF OFFICERS AND DEPARTMENT DESIGNATED MANAGERS

BACKGROUND

The Council allows employees to use the internet facilities for personal transactions during lunch breaks and outwith working hours. All employees who have internet access have been issued with a copy of the Council's Internet Guidelines. This is also readily available on the intranet (see http://webstats/personnel/ , click Employment Matters, click Employee Responsibilities, and click Computer, E-mail and Internet Guidelines).

The Guidelines clearly identify examples of unacceptable use of the internet resources. The Council wants to ensure that employees are discouraged from accessing inappropriate web sites and has consulted with the Trade Unions on the following monitoring procedure. If employees access sites which could lead to criminal prosecution such as child pornography or are of an inappropriate nature, e.g. issues such as firearms, violence, explosives etc, the Council will notify the Police and co-operate with their investigative process. It is therefore necessary that Chief Officers and Department Designated Managers follow these guidelines and give due regard to the Data Protection Acts, the Regulation of Investigatory Powers (Scotland) Act, and the Council's own Harassment Policy when dealing with the monitoring information.

DEPARTMENT DESIGNATED MANAGER

The Department Designated Manager will be a second tier Manager who is identified by the Chief Officer as the person responsible for monitoring the internet violation reports which IT make available to each Department on a monthly basis. In larger Departments, it may be considered appropriate to nominate more than one Department Designated Manager but, due to the sensitivity of the information, they should all be second tier Managers.

It will also be appropriate for each Department to make arrangements for another second tier Manager to cover these particular responsibilities during periods of leave or absence. An up-to-date list of the names of the Department Designated Managers will be held by the IT Designated Manager, as information will only be supplied and/or discussed with authorised Department Designated Managers.

MONITORING PROCEDURE

1. On a monthly basis, IT will inform the Department Designated Manager(s) that reports on internet violations are available for on-line viewing within each Department.

2. The Department Designated Manager will consider the content of the report. If the sites which have been accessed are appropriate for the type of work the individual is carrying out, e.g. an officer accessing a site on cannabis when he/she is dealing with a disciplinary case relating to cannabis, no action is taken.

3. If the Department Designated Manager identifies a suspected inappropriate site, e.g. a site whose title suggests sex, violence, firearms etc issues, he/she will advise their own Chief Officer and the Designated IT Manager.

4. Following discussion with the Department Designated Manager, IT will generate a report on the sites accessed by the employee in the past month and forward it to the Department Designated Manager. The designated Manager and the IT Designated Manager will discuss its content and consider whether or not it is appropriate to contact the Police to request further investigation.

5. Police will investigate the site(s) and report back indicating whether or not they wish to investigate further. In the event that they do, the IT Designated Manager will notify the Chief Executive, the Head of IT, the Assistant Chief Executive (Management) and the Chief Officer of the Department concerned. See Police Investigation section below.

6. In the event that they do not, the IT Designated Officer will notify the Department Designated Manager who will access the same sites and review the content of the sites for possible disciplinary action.

7. The Department Designated Manager will, if necessary, initiate appropriate action in consultation with the Assistant Chief Executive (Management).

POLICE INVESTIGATION

1. The Police will contact the Chief Officer of the Department directly to dscuss their requirements for the investigation. This could entail access to the computer hardware, access to the premises etc.

2. Depending on the circumstances of the investigation, it may be necessary to leave the employee in post until the appropriate evidence has been secured. The Department Designated Manager will discuss the appropriate timing for investigatory meetings and the possible suspension of the employee with the Assistant Chief Executive (Management).

3. All Police requests will be routed through the Department Designated Manager or a more senior officer.

4. The awareness and the detail of the Police involvement will be restricted to only those who <u>need</u> to know.

Appendix 2

INTERNET VIOLATIONS – GUIDELINES FOR THE IT DESIGNATED MANAGER

BACKGROUND

The Council allows employees to use the internet facilities for personal transactions during lunch breaks and outwith working hours. All employees who have internet access have been issued with a copy of the Council's Internet Guidelines. This is also readily available on the intranet (see http://webstats/personnel/ , click Employment Matters, click Employee Responsibilities, and click Computer, E-mail and Internet Guidelines).

The Guidelines clearly identify examples of unacceptable use of the internet resources. The Council wants to ensure that employees are discouraged from accessing inappropriate web sites and has consulted with the Trade Unions on the following monitoring procedure. If employees access sites which could lead to criminal prosecution such as child pornography, or are of an inappropriate nature e.g. issues such as firearms, violence, explosives, etc, the Council will notify the Police and co-operate with their investigative process. It is therefore necessary that if the IT Designated Manager becomes aware that inappropriate sites are being accessed, that they follow these guidelines and give due regard to the Data Protection Acts, the Regulation of Investigatory Powers (Scotland) Act, and the Council's own Harassment Policy when dealing with the monitoring information.

There are guidelines available for IT Department staff and staff in employed in other Departments whose main responsibilities are to provide IT support for their own Department. (Please see Appendix III attached)

The IT Designated Manager is the employee based within the IT Department who is the authorised contact with the Police for the purposes of investigating internet violations.

MONITORING PROCEDURE

1. You will ensure a monthly violations report is provided for the Department Designated Manager(s) in each Department.

2. If while you are processing the information you become aware that there are titles for sites which suggest sex, violence, firearms etc subject matter you will raise this with the appropriate Department Designated Manager. However, it is not your responsibility to monitor the reports.

3. A Department Designated Manager may ask for a user access report for any month. You will identify possible inappropriate sites on this report and discuss them with the Department Designated Manager.

4. If the Department Designated Manager and yourself consider that there is need for further investigation you should advise the Police (i.e. the Duty Detective Inspector on 591901 or 591902).

5. The Duty Detective Inspector will arrange for the sites to be investigated and will advise whether or not they wish to investigate further. If they do, see Police Investigation section below. You will advise the Chief Executive, the Assistant Chief Executive (Management), the Head of IT and the Chief Officer of the Department.

6. If the Police do not consider a criminal investigation is necessary, you will then inform the Department Designated Manager that he/she can access the sites to gather information which he/she requires in order to consider whether it is appropriate to initiate the disciplinary action.

7. You may be required to provide further monitoring data to allow the Department Designated Manager to investigate the breach of the Council's Policy on Access to the Internet.

8. You may be required to assist the investigative process by interpreting the data provided, e.g. provide explanations about the lay-out of reports etc.

9. You may be required to be a witness at any subsequent disciplinary hearings.

POLICE INVESTIGATION

1. If the Police decide to further investigate the access to sites, you will be required to assist by providing information as directed by them.

2. You should keep the Head of IT apprised of your involvement in the investigation.

3. Once the Police have completed their investigation, if appropriate the Council will initiate the disciplinary procedure. You will provide and explain the detail of monitoring information, but you will not access sites which are the subject of Police investigation during the investigatory meetings. You will be a witness at any subsequent disciplinary hearing and legal proceedings.

Appendix 3

INTERNET VIOLATIONS – GUIDELINES FOR IT DEPARTMENT STAFF AND 'IT' STAFF EMPLOYED BY OTHER DEPARTMENTS

BACKGROUND

The Council allows employees to use the internet facilities for personal transactions during lunch breaks and outwith working hours. All employees who have internet access have been issued with a copy of the Council's Internet Guidelines. This is also readily available on the intranet (see http://webstats/personnel/ , click Employment Matters, click Employee Responsibilities, and click Computer, E-mail and Internet Guidelines).

The Guidelines clearly identify examples of unacceptable use of the internet resources. The Council wants to ensure that employees are discouraged from accessing inappropriate web sites and has consulted with the Trade Unions on the following monitoring procedure. If employees access sites which could lead to criminal prosecution such as child pornography, or are of an inappropriate nature e.g. issues such as firearms, violence, explosives, etc, the Council will notify the Police and co-operate with their investigative process. It is therefore necessary that if IT staff become aware that inappropriate sites are being accessed that they follow these guidelines and give due regard to the Data Protection Acts, the Regulation of Investigatory Powers (Scotland) Act, and the Council's own Harassment Policy when dealing with the monitoring information.

There are guidelines available for IT Department staff and staff employed in other Departments whose main responsibilities are to provide IT support for their own Department. (Please see Appendix III attached)

The IT Designated Manager is the employee based within the IT Department who is the authorised contact with the Police for the purposes of investigating internet violations. The IT Designated Manager is contacted on extension 8184.

PROCEDURE FOR IT STAFF BASED IN COUNCIL DEPARTMENTS OR IT DEPARTMENT STAFF WORKING IN CLIENT DEPARTMENTS

1. If, as a result of working on an employee's PC, you suspect that he/she has been accessing inappropriate material, do no further work on the PC in question.

2. Turn off the PC at the power switch of the PC.

3. Do not remove any cables.

4. Contact the IT Designated Manager on extension 8184.

5. Try not to alert the user or his/her colleagues. Remember that there is the possibility that a colleague may have used his/her password.

6. Advise the IT Designated Manager, who in turn will advise the appropriate Department Designated Manager.

7. Do not discuss the matter with anyone else.

8. You may be required to co-operate with any subsequent investigation into the history of the usage of the PC.