TEESDALE DISTRICT COUNCIL

INTERNAL AUDIT SERVICE

INTERNAL AUDIT REPORT

REPORT ON:	ICT
AGREED WITH:	Helen Finnimore

CONTENTS **Section**

Auditor: **John Horsman**
Date Issued:

1.0 INTRODUCTION

1.1 The audit examined the ICT system.

1.2 The audit work was undertaken during April / May 2008.

1.3 It should be noted that the establishment of adequate control systems is the responsibility of management, and that an internal audit review is conducted on a test basis and cannot therefore review every transaction. Thus, while the implementation of internal audit recommendations can reduce risk, and may lead to the strengthening of these systems of control, responsibility for the management of these risks remains with the service manager.

2.0 EXECUTIVE SUMMARY

The majority of the ICT audit was covered through interview and demonstration with Helen Finnimore and Paul Jobson. The controls in place are, on the whole, adequate; many of the more important security arrangements are externally sourced, contracted to an excellent standard. Most of the recommendations are based around policies; the staff are aware of the required action in most cases, however the procedures are not always formally in place. Some aspects, such as the position of the server room (below a kitchen etc) are not ideal, however it is a low probability risk, and it would be unrealistic to expect any major works so close to LGR. I can conclude that the major systems and controls are sound, with only the more minor aspects requiring amendment.

OPINION

The overall audit opinion of the current systems for ICT is that they are ***satisfactory***.

4.0 RISK ASSESSMENT OF WEAKNESSES

Finding Reference	Risk	Probability Score	Probability Commentary	Impact Score	Impact Commentary	Overall Score
3.05	Ex-employees still have access to the system.	4	All ICT staff have knowledge of passwords and so on. Certain circumstances may delay the changing of security arrangements. May happen occasionally and has happened in the past.	5	Potential severe financial loss, damage to the service objectives and capability. Possible adverse publicity.	20
3.06	ICT staff are not up to date with the latest information or procedures.	4	Taking into account the length of time since previous training, it is probable there are more up to date techniques, information and so on available.	1	Minimal impact on service delivery and the meeting of objectives.	4
3.07	Contractors act unscrupulously or provide an unsatisfactory service.	2	Unlikely to occur, not known to have happened previously.	3	Potential disruption to the service and financial loss.	6
3.21, 3.36, 3.37, 3.38, 3.47, 3.48	Server room accessed in order to gain physical access to hardware or data.	4	During the hours of 9-5, the server room remains open. There is a wide window of opportunity, should someone wish to gain entry.	5	There is potential for severe financial loss, adverse national publicity and inability to fulfil objectives.	20
3.38	Weaknesses identified through breaches of security may not be fully controlled or addressed if not recorded in a log.	2	May only occur in certain circumstances and not expected to occur.	4	Service objectives compromised impairment to the service capability.	8
3.38	The extent of data or hardware damage arising from security breaches that are	3	Without formal procedures there is potential for a crucial	3	Disruption to the service, potential financial loss and adverse publicity.	9

Finding Reference	Risk	Probability Score	Probability Commentary	Impact Score	Impact Commentary	Overall Score
	not addressed may be exacerbated.		factor to be neglected.			
3.39	Fire in server room goes unnoticed.	5	Without an alarm, unless someone happens to be present, it is certain a fire would go unnoticed.	4	Inability to fulfil objectives, significant impact upon the service capability. Major financial loss.	20
3.41	Staff unable to control a smaller blaze effectively.	3	Extinguishers are available, although not all staff are trained in using them.	3	Disruption to the service, financial loss, disruption to the service.	9

5.0 ACTION PLAN

	Recommendation	Ranking	See Para	Management Response	To be actioned by: Name	Date
5.01	Ensure the policy specific to ICT staff is implemented. Regular updates of any leavers to be sent to ICT staff and any other relevant staff, if no changes, confirmation to that effect.	Essential	3.05	The formal policy will be finalised / amended and implemented.	**Helen Finnimore**	**06/08**
5.02	Consider enrolling staff on refresher/updated training.	Useful	3.06	This is implemented. Staff training is regularly reviewed, especially with LGR upcoming.	**Helen Finnimore**	**Ongoing**
5.03	Implement a formal procedure to deal with the recruitment, selection and supervision of contract staff.	Important	3.07	The formal policy will be finalised / amended and implemented.	**Helen Finnimore**	**06/08**
5.04	Ensure the server room is physically locked at all times.	Essential	3.21, 3.36, 3.37, 3.38, 3.47, 3.48	This has been implemented.	**Helen Finnimore**	**N/A**
5.05	Ensure staff are aware of action to take should there be a security breach. Formalise written procedures.	Important	3.38	An addendum will be made to the current ICT policy.	**Helen Finnimore**	**07/08**
5.06	Consider installing fire alarms.	Essential	3.39	An assessment will be made upon the reasonableness of this action.	**Helen Finnimore**	**07/08**
5.07	Consider providing staff fire training.	Important	3.41	The health and safety officer is to be contacted and consulted for advice.	**Helen Finnimore**	**07/08**