ITEM 8

The Gateshead Housing Company
Working with Gateshead Council

AUDIT COMMITTEE

1 July 2015

PRESENT:

Directors
George Clark (Chair)
Robert Buckley
Mick Davison
Helen Hall
Joachim Moussounda Mouanda
Peter Mole

Advisers

Jon Mallen-Beadle	Managing Director
Neil Bouch	Director of Customers and Communities
Natalie Hewitt	Head of Corporate Services
Phil Gallagher	Head of Investment and Development
Kevin Johnson	Head of Customer Services
Stuart Gibson	Governance and Risk Officer

Also in attendance

David Johnson	Chief Internal Auditor, Gateshead Council
Jane Wright	Audit and Risk Manager, Gateshead Council
Nick Plumb	KPMG
James Morgan	KPMG

Apologies
Tracy Harrison

38 MINUTES

The minutes of the meeting of the committee held on 22 April 2015 were approved as a correct record.

39 REPORT ON THE STATEMENT OF INTERNAL CONTROL – 2014/15

It is a requirement under the UK Corporate Governance Code that companies undertake, at least annually, a review of the effectiveness of their systems of internal control. A company's board should undertake this review for the purposes of making its public Statement of Internal Control, which is published as part of the financial statements.

The statement of internal control as published as part of the financial statements was submitted, covering the following areas: -

- Governance and Risk Management

- Performance Management
- Financial Management
- Internal Audit
- External Audit

The report is designed to provide assurance that the information, as stated within the statement of internal control, is accurate and reliable and can be published as part of the financial statements.

RESOLVED – (i) That the Board be recommended to approve the Statement of Internal Control contained within the Financial Statements for the year ended 31 March 2015.

(ii) That Helen Hall be provided with a copy of the Langlands Report.

(iii) That the committee place on record its congratulations to all employees for receiving a clean bill of health.

40 DRAFT DIRECTORS' REPORT AND FINANCIAL STATEMENTS – 2014/15

The committee received the report and financial statements, as agreed with the auditors, KPMG, for the year ended 31 March.

The financial result for the period was a surplus of £546,000 (2014: £621,000 deficit).

The fourth quarter management accounts indicated that the financial result was an expected surplus of £413,000, however it was subsequently agreed that the Repairs and Maintenance budget surplus of £158,000 would be returned to the Council.

This was then offset by an additional £21,000 of repairs costs that required accruing and an increase in the FRS 17 adjustment from Aon Hewitt in relation to Pension Scheme Finance Costs (£500,000).

The company achieved a pre-tax and interest surplus in the year of £44,000 prior to interest receivable of £2,000 and pension scheme finance income of £500,000 (2014: interest receivable of £4,000; finance costs of £50,000).

The balance sheet has been increased due to the surplus, resulting in closing revenue reserves excluding net pension provisions of £1,066,000 (2014: £830,000). The directors and management continue to implement efficiency savings ahead of targets and as a result believe the company is in a strong financial position to deliver its strategic and operational goals.

In line with last year's accounts, it has been necessary under FRS 17 (a financial reporting standard) to adjust the accounts for the pension fund liability attributable to the company's employees. The net pension liability was £11.71m as at 31 March 2015 (£7.75m as at 31 March 2014) as calculated by the Pension Fund's actuary.

The committee queried why less interest had been generated than last year despite there being more money in the bank. The Managing Director agreed to look into this and report back to the committee.

The committee asked for an explanation why the pension fund was so different during the last two years. It was noted that there was no simple explanation, however it was primarily due to the gift yield in each year.

RESOLVED – That the Board be recommended to approve the Directors Report and Financial Statements for the year ended 31 March 2015.

41 KPMG MANAGEMENT REPORT – YEAR ENDED 31 MARCH 2015

The committee received the external auditor, KPMG's management report on the financial statements for the year ended 31 March 2015.

There were no significant issues raised in the report and all of the recommendations have been responded to by the Company.

As part of the audit, KPMG require the letter to be signed by the Chair and the Company Secretary on behalf of the Board, a copy of which was submitted.

When KPMG presented its management report for the year ended 31 March 2014, the committee requested that future reports also include a glossary of terms/abbreviations. It was agreed that this would be added to the report.

RESOLVED – (i) That the management report for the year ended 31 March 2015 be approved, subject to the inclusion of a glossary of the terms/abbreviations.

(ii) That the Board be recommended to authorise the Chair and the Company Secretary to sign the management representation letter on behalf of the Board.

(iii) That the financial performance be presented in a more understandable format in future reports.

(iv) That the committee place on record its thanks to the TGHC Finance Team for receiving such a good bill of health with only one minor recommendation.

42 OPERATIONAL RISK REGISTER

An updated Operational Risk Register for the Corporate Services and Customers & Communities Directorates was submitted.

The following risk has been added to the register following a recommendation made by Internal Audit during its audit of VAT arrangements: -

Finance

- Incorrect treatment of VAT could lead to fines and interest payments to HMRC

The following risk has been updated to a green risk and will be monitored internally: -

Investment Works

- Increase in complaints from customers, councillors and other stakeholders.

The following risk has been deleted from the register as it is no longer considered an issue: -

Lettings

- Lack of availability of properties in demand.

The committee expressed concern about the residual scores of the some of the repairs risks relying on the BARIS interface given that no date was provided for implementation. It was noted that while a work around is in place and testing of the Baris interface was ongoing the benefits of integration had not yet been realised. The Company is continuing to work with the Council's Construction Services and ICT supplier on the solution.

RESOLVED – That the updated operational risk registers for the Corporate Services and Customers & Communities Directorates be approved.

43 ICT SECURITY POLICY

The Board approved an ICT Security Policy in 2008 to ensure that all users of the Company's ICT systems were aware of the security risks that were always present.

Following an internal audit report in March 2012, and in the face of changing technology and working practices, it was found that TGHC needed to review its ICT Security Policy.

Internal Audit reviewed the ICT Security Policy, the Computer Security Policy and the Internet and Email Policy and found conflicting statements in relation to the disposal of data storage equipment and also in relation to the use of personal email and internet. This was resolved and an updated Policy was rolled out to all employees in September 2012.

In June 2015, the TGHC ICT Development Team was realigned to better meet the needs of the company and responsibilities redefined, with ownership of the ICT Security Policy now lying with the ICT Development Manager.

The ICT Security Policy has therefore been reviewed and the updated ICT Security Policy was submitted.

As part of a wider schedule of information governance, the ICT Security Policy will be reviewed and updated annually.

RESOLVED – That the Board be recommended to approve the updated ICT Security Policy, which is attached as an Appendix to these minutes, and the policy be reviewed annually.

44 SENIOR INFORMATION RISK OFFICER (SIRO) ANNUAL REPORT

Following an internal audit report in November 2013, it was found that TGHC needed to manage risks associated with its information assets in the same manner that other corporate risks were managed. To ensure the ongoing management of information risk, a Senior Information Risk Officer (SIRO) role was created and delegated to Andrew Curtis, ICT Development Manager.

It was also agreed that the SIRO would work with the TGHC Governance Officer to ensure that any risk management procedures were compatible with the current corporate approach and incorporated into existing policies and procedures. Risks would be identified and assessed and added into the current risk register.

A review of information risks across TGHC was carried out by the SIRO and Governance Officer. 16 Information Assets were identified and agreed as risks across TGHC, details of which were reported.

A risk assessment was carried out for each risk using the four scale matrix, to assess impact and likelihood, in line with other TGHC Risk Registers.

A summary of the information asset risk scores in consideration of pre and post mitigation measures and details of the Information Asset Owner for each Information Asset were submitted.

The Risk Assessment Task List for areas where further mitigation has been identified was also submitted. Each outstanding task has been delegated to a specific task owner with a forecasted completion date.

RESOLVED – That the Information Asset Risk Register be approved and updates be brought back to future committees.

45 INTERNAL AUDIT ANNUAL REPORT 2014/15

The committee received details of the work undertaken by the Internal Audit Service for 2014/15 and an overall assessment of the adequacy of the Company's internal control systems based on this work.

The position for the year highlights the completion of 132% of the audit plan, in terms of actual audit hours against planned hours (123% for 2013/14). Details of other relevant performance information were also reported.

The 2014/15 Internal Audit Plan agreed 20 audits to be carried out in the year. All audits have now been fully completed with the exception of one which is currently at the draft report stage.

Of the 20 planned audits for 2014/15, 18 concluded that systems and procedures in place were operating well or satisfactory, one audit was a follow-up audit and an opinion was not required and one audit is still issued in draft.

Internal Auditors have received full co-operation from all employees involved in the areas under review and all audit recommendations have been satisfactorily addressed by management.

The Chief Internal Auditor has in place a quality review process which appraises external assessment against Public Sector Internal Audit Standards (PSIAS), self-assessment against the CIPFA Statement on the Role of the Head of Internal Audit, reliance placed upon Internal Audit by the Council's external auditor and assessment of the effectiveness of the Audit Committee and relevant performance information.

For the year ended 31 March 2015, the Internal Audit Service has been externally assessed against Public Sector Internal Audit Standards. This assessment was undertaken by external audit.

The outcome of the assessment was positive and found that the Internal Audit Service is substantially compliant with the standards in all significant aspects and that there are no areas of concern that the Internal Audit Service is unable to form a judgement as to the proper and effective working of the system of internal control.

RESOLVED – (i) That the committee is satisfied with the Internal Audit Annual Report 2014/15.

(ii) That the committee placed on record its thanks to the Council's Internal Audit Service for its work during the year.

46 2015/16 INTERNAL AUDIT PLAN – PROGRESS REPORT

Progress made by the Internal Audit Service against the audit plan for the financial year 2015/16 was reported.

As at 19 June 2015, one final report has been issued and two further audits were in progress.

RESOLVED – That the committee is satisfied with progress to date with the 2015/16 Internal Audit Plan.

47 FORWARD PLAN

A forward plan of reports which will be presented to Audit Committee during the next year was submitted.

RESOLVED – That the forward plan be noted.

48 DATE AND TIME OF NEXT MEETING

The next meeting of the committee will be held on Wednesday, 14 October 2015 at 2pm in Room S21, Gateshead Civic Centre, Regent Street, Gateshead.

49 EXCLUSION OF THE PRESS AND PUBLIC

RESOLVED – That the press and public be excluded from the meeting during consideration of the remaining business in accordance with Category 4 of the Company's Access to Information Rules.

Appendix

The Gateshead Housing Company
Working with Gateshead Council

Information and Communication Technology

Security Policy

Date Updated: June 2015

Version number: 3.0

Owner: Andrew Curtis

Introduction by the Managing Director

The Company recognises that Information and Communications Technology (ICT) is an essential tool used to provide effective and efficient services. Information held within ICT systems is a key resource and we have to make sure that it is used appropriately and securely, and that the Company is protected against potential security threats. The revised ICT Security Policy sets out the Company's approach to ICT security. It is intended to help employees to understand the implications of using ICT and their responsibilities in relation to its use.

It is important that we all take our responsibilities seriously, as we want everyone to be able to work with the many types of technology that are now classed as ICT in a safe and secure environment. All employees are responsible for making sure that the policy is put into practice.

Please read this policy and if there is anything you don't understand, please talk to your supervisor or manager.We are sure that with the co-operation of everyone, this policy will improve ICT security throughout the Company.

J Mallen Beadle

The Gateshead Houisng Company Managing Director Jon Mallen Beadle

ICT Security Policy

Introduction

The use of Information and Communication Technology (ICT) helps the Company to provide effective and efficient services and is a vital tool in the work of many employees. To ensure that the Company obtains the most benefit from ICT, users must understand and comply with their responsibilities in relation to the secure use of ICT resources and the information held within them.

This policy is designed to ensure that all users of the Company's ICT systems are aware of the security risks that are always present. As such, it is intended to help protect the Company's information from all threats whether internal or external, deliberate or accidental.

This policy is based on the ISO 17799 & 27001 standards for information security, which contain comprehensive sets of security controls to improve the level of security within the organisation. The adoption of these controls provide a firm indication that the Company is taking "due care" of information which is one of the basic requirements of the Data Protection Act 1998.

In addition to this policy, a wide-ranging set of Standards, Procedures and Protocols governing the use of the Company's ICT is available on the Intranet. Users must be familiar with, and adhere to, the relevant sections contained within them.

Why is this Policy important?

Users who fail to follow the policy risk causing major disruption to Company business,may incur large fines from the Information Commissioner and cause damage to the Company's reputation. Such misuse could result in disciplinary action and/or legal action

Who does the Policy apply to?

The policy applies to any user of Company Information Systems:

- Agency workers
- Board and Committee Members
- Contractors
- Employees
- Employees of 'partner' organisations
- External auditors
- Inspectors
- Temporary workers
- Visitors
- Voluntary sector workers
- Work placements

What is ICT equipment?

For the purposes of the policy, ICT equipment is defined as being: "Any item of electronic equipment that is capable of storing or transmitting Company information". This includes, but is not limited to, technologies such as:

- Audio recording
- CCTV
- Computers
- E-mail systems
- Fax machines
- Internet access
- Mobile phones

- Smart Phones
- Mobile radios
- Network equipment and cabling
- Photocopiers
- Photographic equipment
- Printers
- Scanners
- Tablet Devices
- Telephones
- Video conferencing
- Video recording
- Web cameras

Users must contact ICT Services before procuring any items of ICT equipment or software. ICT Services will ensure that all items meet Company standards, are secure and are compatible with existing systems.

Computer Security

Deliberate unauthorised use of passwords, attempts at unauthorised access to the network and systems, together with the unauthorised alteration of data are all offences under the Computer Misuse Act 1990.

To ensure compliance with the law and Company policy users must:

- not access or attempt to access any files, folders, logs, reports, messages, systems or information without authorisation.
- never let anyone else know their password. Users should inform their line manager if they have reason to believe that someone knows their password.
- not access a computer system using someone else's username and password for any purpose
- not make or attempt to make any changes to the operating system or settings on Company computers.
- not install, attach, insert, connect, attempt to connect or remove any item of equipment to or from a Company computer or the Company network without prior authorisation from ICT Services.
- obtain written permission from their line manager before taking and/or using Company owned equipment anywhere other than their normal work location.
- ensure that all ICT business application procurements and solutions (including externally hosted systems) are procured via Corporate Procurement and that all other computing equipment, peripheral devices and software to be used for Company business purposes are procured via ICT Services.
- Regardless of whether the procurement has taken place through Corporate Procurement or ICT Services all orders for ICT related goods and services must be placed via ICT Services.
- be authorised before using Company equipment

Personal use of Company ICT equipment

Personal use of Company computing equipment is allowed, however:

- It must:
  - Occur within a user's own time (i.e. when keyed out of the flexi system or during a lunch break) – please note that there is a separate section covering personal use of the Internet

- It must not:

- Interfere with the performance of a user’s duties
- Take priority over work responsibilities
- Result in the Company incurring financial loss
- Bring the Company into disrepute
- Be unlawful or contrary to Company policy or Code of Conduct
- Be for private business purposes

- Company equipment may be used to prepare simple documents or spreadsheets on personal matters such as a letter to a bank or utility provider. Personal documents should only be stored temporarily on the Company’s computers whilst they are being prepared and should be deleted from the system after completion.
- Users are allowed to use Company equipment to print a limited number of personal documents. Users must pay for all printing in line with a scale of charges. (See TGHC Admin for details)
- The printing of photographs and images is not allowed.
- Company equipment must not be used for playing games, music, videos etc.
- Personally owned ICT equipment must not be connected to the Company network or computers.
- All redundant items of computer equipment and storage media such as floppy discs, DVD’s, CD’s, tapes etc. must be returned to ICT Services for secure disposal.

Portable Storage Devices

The following list includes examples of portable storage devices but is not limited to:

- Laptop and Notebook PC’s
- Handheld equipment – for example, PDA’s; Smartphones, ‘Blackberries’
- Tablet Devices
- USB memory sticks
- Flash memory cards
- Floppy disks
- CD’s & DVD’s
- Portable hard drives

Guidelines for use of Portable Storage Devices

- If a portable storage device is lost, stolen or mislaid it must be immediately reported to the users line manager and ICT Services.
- Only encrypted memory sticks may be used on company equipment.
- Portable devices must be stored securely when left unattended. Additionally, devices taken off-site should not be left unattended in public places, including clients’ homes.
- Portable storage devices must not be used to store sensitive, confidential or personally identifiable information without prior consultation with ICT Services.
  ICT Services can offer advice on the best method of securing data against the risks of loss and / or disclosure.
- Users must obtain approval from their line manager before creating, moving or copying information, files, folders etc onto a portable storage device.
  A list of files stored on the portable device should be kept in case the device is lost or stolen.
- Information held on portable storage devices is not automatically copied (‘backed-up’). To avoid total loss of data, users must ensure that information stored on portable storage devices is ‘backed-up’ by connecting to the Company’s ICT network and storing the files on a networked drive.
- Company computer equipment must not be connected to any computer network other than the Company’s, unless specifically approved by ICT Services.
- Only authorised Company employees may use Company owned portable

equipment.

- Care should be taken to ensure that display screens can not be overlooked.
- Users who are issued with a laptop must ensure that it is logged on to the network at least once a month to allow the anti virus software to be automatically updated. Users who are issued with a laptop and do not know when it was last connected must take it to ICT Services for a manual update before using it.
- If a portable storage device is lost, stolen or mislaid it must be immediately reported to the user's Service Operational Risk Co-ordinator
- Visitors or contractors who bring their own USB devices into the Company (to give a presentation for example) should be supervised at all times whilst the device is connected to Company equipment

Housekeeping

- Business data and files should be saved on a shared network drive in accordance with the Company's Information Management Policy. This will allow other users to access the information in your absence. The H:\Drive should not be used to store such data.
- Users must ensure that their file and folder permissions should be set to permit access only to employees who have a relevant business need. Please contact ICT Services for advice on how this should be done.
- Users must ensure that sensitive or classified information is not left on view or lying on desks whilst unattended.
- All Company computers must be left with a clear screen whilst unattended. Computers will automatically lock after 10 minutes of inactivity to enforce this policy, however users should 'lock' the screen whenever they leave their desks (using ctrl/alt/delete) even for short periods of time.
  If the computer is to be left unattended for long periods, users should 'log-out'.
- Sensitive or classified information should be cleared from printers, fax machines, copiers, scanners etc immediately.
- Computer printouts and any other documentation no longer required must be disposed of in a controlled and secure way.
- Computer equipment that is not being used for long periods, overnight and at weekends for example, should be switched off to conserve energy and may be automatically shutdown via company hibernation software.

Software

- All software (including fonts, shareware and freeware) to be used on Company computers must be procured and installed through ICT Services.
- All computer software must be used in accordance with its licence agreement.
- All software must be catalogued and held centrally by Gateshead Council ICT Services to ensure compliance with FSSC-1, the Federation Against Software Theft (FAST) Standard for Software Compliance.

Anti Virus Precautions

- All incoming e-mails are scanned for viruses before they reach a users 'Inbox'. However because new viruses are created almost daily, it is important that users are cautious at all times. All e-mails, especially those with attachments, could be a risk. If there is any doubt, users must contact the ICT Service Desk before opening e-mail or attachments
- Files on Floppy disks, CDs, DVDs or USB memory sticks are automatically scanned for viruses as they are opened.
- Users who get a virus alert from anywhere other than ICT Services should inform the ICT Service Desk.
- Do not forward a virus alert message to anyone else.

Internet Access

The Internet can be a very useful tool for getting information quickly and easily. However access to the Internet also presents a number of risks to both the Company and users. This policy defines what is acceptable, what is not acceptable and what controls must be followed when using Company equipment to access the Internet.

Specific requirements

The following requirements apply to all use of the Internet, both for Company purposes and personal use using Company equipment:

- Users must not intentionally access or attempt to access information or images that are obscene, sexually explicit, racist or defamatory or which depict violent or criminal acts or otherwise represent values that are contrary to Company policy
- All access to the Internet must be via a method approved in advance by ICT Services
- Users must not access or attempt to access Internet based file sharing networks, typically used for downloading and sharing music and video files. If you are in any doubt you must contact ICT Services for advice before attempting to access any website.
- A user who accidentally opens a website showing material that breaches Company guidelines must exit the site immediately and report it to the ICT Service Desk without undue delay.
- Any user who tries to access a website that is thought to be within Company guidelines but finds that it is blocked should ask for it to be unblocked using the form on the Web Blocking page.

Purchasing online

Users must not acquire or buy any goods or services for Company business purposes directly from web sites or other Internet sources. Users should first contact Corporate Procurement for confirmation that they are complying with the latest procurement procedures.

Copyright

Much of what appears on the Internet is protected by copyright. This can include images and logos, as well as documents and information. The Copyright, Designs and Patents Act 1988 states that only the owner of the copyright is allowed to copy the information and any copying without permission, including electronic copying, is prohibited.

Spyware

Spyware programs interfere with the normal running of a computer and/or collect and transmit potentially sensitive data without the user’s knowledge. These programs are often ‘hidden’ in ‘free’ software offered by websites.

Users must not install or attempt to install any software or web browser toolbars.

Users who suspect that their computer may be infected with spyware should contact the ICT Service Desk.

Personal use of the Internet

Personal use of the Internet is allowed however it must not have a negative impact on the Company by:

- Being unlawful or contrary to Company policy or Code of Conduct
- Bringing the Company into disrepute
- Interfering with the performance of a user’s duties
- Taking priority over a user’s work responsibilities

Personal use is permitted during office hours but must be in the employee’s own time. That is, the employee must be clocked out if they are using the internet for personal use, and this must not interfere with the performance of a users duties.

Users who do not have access to a company computer can gain access to the Internet on one of the Company's public Internet access facilities during their own time. These are located at all libraries and the Civic Centre.

Personal use - What Users CAN do

- Access browser based personal e-mail systems (for example, log on to webmail to check personal e-mail)
- Browse web pages, (check the latest news, research a hobby, bank online for example)
- Buy goods and services online for personal use where a download to the computer is not required (shop online, book a flight or holiday, use online auction sites for example)
- Print information – a limited amount of personal printing is allowed. Users will be charged for personal printing in line with a scale of charges. (See the Intranet for details)

Personal use - What Users CAN NOT do

- Access Chat Rooms
- Access streaming media (including radio and television)
- Buy music, video etc if it requires a download
- Change settings on Company computers
- Create or update a personal website
- Download and / or upload software, images or files
- Download or play games
- Download or play music or videos
- Have goods or services bought online delivered to the workplace
- Use Instant Messaging or Web Messaging
- Use a Company e-mail address to subscribe to websites accessed for personal use
- Use it for private business purposes
- Use it for gambling

The Company uses a number of measures to protect its computers from viruses and spyware etc. However no guarantee can be given that personal details, bank and / or credit card details are secure. Users who choose to enter personal details or buy online do so at their own risk.

Forums

Internet discussion forums can be an effective and efficient method of sharing information and best practice with peer groups and similar organisations. However users must be aware that any comments posted on a forum may be visible to anyone in the world with an Internet connection. Users who join an Internet discussion forum must conduct themselves in an honest and professional manner and care must be taken when disclosing information. All views expressed must reflect the views of the Company and must be in accordance with the Company's Code of Conduct. This applies for both Company business use and personal use of the Internet.

Monitoring

Business and personal use of the Internet is monitored and usernames, websites visited, dates and times of the visits, and the time spent at each site is recorded.

Where there is reason to suspect misuse, management are able to access detailed reports of this information.

Social Media

The use of social media sites is restricted in the company.
Social media includes use of sites such as:

- Facebook
- Twitter
- Google+
- LinkedIn
- Pintrest
- Flickr
- Friends Reunited
- Bebo
- MySpace
- SecondLife
- Yammer

Use of Company Social Media Accounts
Those with access to company sites must abide by the following terms:

- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring The Gateshead Housing Company and its partners into disrepute
- Must not be used for party political purposes or specific campaigning purposes as the councils are not permitted to publish material which 'in whole or part appears to affect public support for a political party' (LGA 1986)
- Must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns
- Must not be used in an abusive or hateful manner
- Must not be used for actions that would put partner representatives in breach of organisations' codes of conduct or policies
- Must not breach partners' misconduct, equal opportunities or bullying and harassment policies
- Any communications with under-18s must be treated with great care and consideration, both to safeguard the young people and also protect the member(s) of staff against any potential allegation, and to avoid any possible misrepresentation of their motives. Logs of communication with all young people should be kept indefinitely on the social media site in case any false allegations are made. The only reasons that communications should be deleted are when there are inappropriate posts by members of the public – and in this case you should keep details of the deleted content offline
- In all broadcasts and communications with young and vulnerable people using social media, regular messages must be used in the social space to inform the users of measures they can take against online harassment and reporting inappropriate online behaviours – for example the Facebook 'panic button'
- Post honest, informative, transparent and respectful comments
- Be human when you comment, judging the content of what you are saying to choose the correct language – try not to be too formal unless the situation demands it but equally do not be too informal if this comes across as unprofessional
- Do not post offensive comments, responses and remarks
- Do not publish anything that damages the reputation of The Gateshead Housing Company
- Respond in a timely fashion to enquiries – monitor the tool regularly and effectively – responses should take no longer than 36 hours. If left dormant it will have an adverse affect on the image of the housing company

- Link to relevant official content on the housing company's website whenever possible
- Do not comment or discuss issues that you are not qualified or suitable to do so – contact the relevant employee for information
- Post comments that are factually correct – avoid arguments and if disagreeing with a point ensure this is done politely and respectfully
- If a complaint is received through a social media platform, this should be dealt with under the company's complaints procedure
- Never consider that discussions are private – conduct yourself as you would face-to-face and, even in a private setting, never post, publish or respond if you would not wish the content to be public
- Never use the social media tool outside work in your housing company capacity
- Do not accept interaction or requests from people with offensive, inappropriate names and/or images associated with them
- Never ask for personal information via social media in a publicly-available space. If you do receive any such information note the content of it, delete it from public view
- Consider copyright – do not post any information or other material which is copyright-protected, without permission of the copyright owner

Use of Personal Social Media Accounts

Outside the workplace, your rights to privacy and free speech protect online activity conducted on your personal social networks with your personal e-mail address. However please consider the following:

- However, what you publish on such personal online sites should never be attributed to the company and should not appear to be endorsed by or originated from the firm. If you choose to list your work affiliation on a social network, then you should regard all communication on that network as you would in a professional network. Online lives are ultimately linked whether or not you choose to mention the company in your personal online networking activity. Don't disclose confidential information through any medium.
- Do not use your housing company e-mail address to set up any social media account.
- For your own protection you should set your privacy settings so that only your friends can see your details; and never accept communications with under 18s that you have dealt with in a professional capacity. Remember that these sites are often monitored by the police.
- Please remember that any behaviour that may cause offence to others has the potential to put your employment in jeopardy.
- Remember that comments posted on social networking sites may be difficult or impossible to remove

E-mail

Whilst e-mail may often appear to be an informal method of communication users should remember that it has the permanence of written communication, and as such users must ensure that it meets the same standards as other published documents.

All e-mail and attachments sent and received on Company equipment (including personal e-mail) are owned by the Company. When using e-mail as a means of communication users should be aware that:

- Advice given by e-mail has the same legal effect as that given in any written format
- All e-mails are archived and a copy is retained by the Company for a minimum period of 6 months, including those that have been deleted from mailboxes
- All e-mails are potentially subject to disclosure under the Freedom of

Information Act

- E-mail communications, both internally and externally, can not be guaranteed to be private or secure, nor to arrive at their destination either on time or at all
- E-mails may be produced in court in the same manner as any other Company document
- Once an e-mail has been sent there is no control over who the recipient may then forward it on to, either intentionally or accidentally
- The impersonal nature of e-mail messages can mean that it is easier to cause offence than when speaking and attempts at humour can easily be misinterpreted
- Users must not keep e-mails that are construed as business records in e-mail folders. These e-mails should be saved on a shared drive in accordance with the Company's Records Management Policy.

What NOT to do when using e-mail

When using the Company's e-mail system any behaviour or comments that are not permitted in the spoken or paper environment are also not permitted in e-mail messages. Additionally users must not:

- Conduct any business other than that of the Company via e-mail
- Enter into any commitment on behalf of the Company unless explicitly authorised to do so
- Forward chain mail or jokes
- Forward messages unnecessarily
- Generate e-mail in such a way that it appears to have been sent from someone else
- Read, delete, copy or modify the contents of any other user's mailbox without prior authorisation in writing from a Head of Service, unless access has been delegated to that mailbox by the mailbox owner
- Register for automated alerts or subscription services unless there is a valid business reason for doing so
- Send information of a sensitive or confidential nature to any non council e-mail account, without contacting ICT Services for access to the secure e-mail facility provided by ICT Services. If an employee needs access to the Companies e-mail system from home they should contact ICT Services who will arrange for secure access to be set up, subject to authorisation by a line manager.
- Send or forward e-mail that could be construed as obscene, sexually explicit, racist, defamatory, abusive, harassing or which describes violent or criminal acts or otherwise represents values or opinions that are contrary to Company policy. Employees who receive e-mail of this nature should inform their line manager immediately
- Send unsolicited bulk e-mail or Spam
- Use a personal e-mail account for Company business purposes
- Use e-mail to send frivolous messages or gossip
- Use a council e-mail address to subscribe to websites accessed for personal use

Personal use of e-mail

Personal use of e-mail is allowed, however it must not:

- Be unlawful or contrary to the Company's Code of Conduct
- Have a negative impact on the Company
- Interfere with the performance of the user's duties
- Result in the Company incurring expense

- Take priority over work responsibilities

The rules governing business use of e-mail are also applicable to all personal use of e-mail. Users should create a folder named “Personal” within Outlook. Any sent or received e-mail that is of a personal nature should then be moved into that folder. E-mail in this folder will not normally be accessed by others. However others may be allowed access as part of an investigation, or on suspicion of inappropriate or excessive use of e-mail by a user. E-mail relating to Company business must not be stored in the Personal folder.

Access to a user’s mailbox by others

There may be occasions, if a user is away from the office for an extended period for example, when it is necessary for a line manager or a colleague to access e-mail messages in the mailbox of another user. Access to a user’s mailbox may also be granted to action:

- Evidence in a criminal investigation
- Evidence in legal proceedings
- Evidence in support of disciplinary action
- Freedom of Information requests
- Subject access requests under the Data Protection Act

Management of e-mail records in accordance with the Information Management Policy will help to avoid this situation occurring.

Attachments

- To reduce risks associated with e-mail attachments certain file types are prevented from being sent and received on the Company’s e-mail system, for example .exe, .bat, .com, .mp3, .scr etc.
- E-mail with attachments larger than 10Mb will be blocked. Users should note that external organisations may also have attachment size limits on their e-mail systems, which may be as low as 2Mb.

Spam e-mail

Junk e-mail or Spam is a major problem across the Internet. Although the Company's e-mail system blocks tens of thousands of Spam messages every month the large number of such e-mails involved means that some will still get through.

If this happens:

- Do not respond to Spam
- Do not try to unsubscribe from a Spam e-mail – Any response will allow the sender to know that the e-mail address is valid and will probably result in more spam e-mails
- Do not react to false virus reports. These reports tell the user how to take measures against a so-called virus. In reality there is no virus, but following the instructions may damage the computer

Monitoring of e-mail

ICT Services make every effort to ensure the privacy of user data, including e-mail messages. Any information obtained by ICT Services during the course of systems administration will be treated as confidential and will not be used or disclosed in the normal course of events. Where routine systems management (i.e. technical management of the system to ensure that it is operating correctly) or administration indicates a breach of Company policy or the law, ICT Services will bring this information to the attention of the Company or other relevant authorities.

Information Sharing

Where it is necessary to share personal or organisationally sensitive data with another organisation and the other organisation provides (for example) a secure web site or similar facility specifically for the upload of the data to be shared, then this facility must be used by Company employees.

If it is necessary otherwise to send information of a personally identifiable or sensitive nature by email to an external recipient it must be encrypted and where applicable, digitally signed. Users should note that password protection of a Word document or Excel spreadsheet or putting a CD or USB device in the post is not a secure method of safeguarding data and should not be used to transmit sensitive or confidential data. Please contact ICT Services for advice on encryption of email and digital signatures for this purpose.

Where there is a need to share information and the amount to be shared is too large for email, ICT Services can provide a secure file transfer service (SFTP). This can be used as an alternative to secure e-mail to transfer files containing sensitive or personal information that are too large to either send or receive by e-mail between the Company and other organisations. The facility can be used from any computer with an internet connection to easily and securely upload and download files. Access is controlled by a username and password. If this facility is more appropriate for secure information sharing, please contact ICT Services for advice on its use.

Telecommunications

Users must contact ICT Services before procuring any items of telecommunications equipment or software. ICT Services will ensure that all items meet Company standards, are configured securely and are compatible with existing systems.

Telephone systems

All outgoing calls from Company telephone systems are logged. The log records the date and time of the call, its duration, the extension that was used to make the call and the number called.

When using a Company telephone, users should take care that the information being discussed is not overheard by passers-by. Users should also be aware of the importance of checking the identity of all callers requesting personal or otherwise sensitive information.

It is accepted that occasionally users may need to make personal telephone calls whilst at work. However, users should make sure that the facility is not abused and that office telephones are not unduly tied up with personal calls.

- It also applies to incoming as well as outgoing personal calls.
- The amount of work time taken up by personal calls must be kept to a minimum.
- This applies to internal and external personal calls.
- Wherever possible personal calls should take place outside work hours, for example during lunch breaks.

In the Civic Centre and where the facility exists at other Company offices all personal calls must be made using the 174 access code and not the 9 access code.

Fax machines

Confidential information can be vulnerable when sent by fax to others. Mail is usually sealed, but faxed documents can be read by anyone who has access to the fax machine. For this reason careful consideration should be given to the positioning of fax machines.

The 'ring ahead and confirm system' should be used especially when faxing confidential or sensitive data. The intended recipient should be called to confirm that a fax will be sent to them and then they should be called to check that it was received. The sending of a test fax prior to sensitive information being transmitted is also recommended.

Users should be aware that the responsibility for the fax lies with the person sending, or asking for the fax to be sent.

Voice mail

When used correctly voice mail systems offer a convenient method for callers to leave non-urgent messages when there is no one available to answer the telephone. It is important therefore that users are aware of the following points in order to ensure the system is used securely:

- Do not use simple number sequences for example 0000, 1111, 1234 etc when creating PIN codes.
- PIN codes must be kept confidential. It must not be disclosed to anyone and should be changed regularly

Mobile phones

The handset and all equipment remain the property of the Company.

A register of use will be kept for those issued with a pool mobile phone. Users should sign the phone ‘out and in’ on the same working day.

All pooled mobile phones should be returned to the relevant section at the end of each working day or shift or as soon as possible afterwards. Phones should be stored in a locked, secure place in the relevant section when not issued.

Users are personally responsible for the security and day to day maintenance of the phone. Losses of handsets or equipment must be reported to the Service Administrative Section immediately. Losses resulting from carelessness may lead to disciplinary action.

The phone must not be used by unauthorised persons.

Private use of the handset is allowed but should be limited to essential calls which must be paid for. Private use will be monitored and any misuse will result in it being withdrawn.

All access to the Internet, television, video, radio and other media, whether for Company business purposes or personal use, must be via a method approved in advance by ICT Services.

Reprographic Equipment

Cameras

As with any other item of ICT equipment, only cameras procured through ICT Services may be connected to the Company network or computers. Personally owned cameras must not be connected.

Printers, Photocopiers & Scanners

Care should be taken to ensure that printing is sent to the correct printer to minimise the risk of unauthorised viewing. Users should ensure that sensitive or confidential information is not left unattended on a printer, photocopier or scanner.

CCTV equipment

All CCTV equipment must be used in accordance with the relevant legislation and in line with the guidelines published on the Information Commissioners web site (http://www.ico.gov.uk/).

Payment Card Security

The Company has developed its Payment Card Industry Data Security Standard Policy and Procedures (PCI Policy) to ensure that the Company and its employees exercise care with the details of payment cards (debit, credit and pre-payment cards) that customers use to make payments to the Company. The policy must be adhered to by all employees involved in processing card transactions or in the support of systems used to do this. The details of the PCI Policy can be found in the Standards and Protocols document that supports this main Information Security Policy document.

Business Continuity

It is the responsibility of individual Groups and Services to ensure that they have business continuity and disaster recovery arrangements in place in support of the ICT systems they operate. Arrangements in support of any corporate ICT elements involved in the system will be the responsibility of ICT Services. Managers in user groups and services should liaise as necessary with ICT Services to ensure their own Business Continuity arrangements for ICT systems used by their service are coordinated with the corporate arrangements of ICT Services

Incident Reporting and Monitoring

Incident Reporting

Any user who knows of a security incident or suspects someone is misusing the Company's computers either deliberately or accidentally must report it to their line manager or e-mail Incident Reporting (incidentreporting@gateshead.gov.uk) as quickly as possible. The line manager is responsible for ensuring that the incident is recorded and the Company's Incident Reporting Group are informed without undue delay.

The procedure for incident reporting is covered in more detail in the Company's Confidential Reporting Code, which is available on the Intranet.

Monitoring of Activity

The Company reserves the right, consistent with the relevant legislation, to exercise control over ICT resources and to monitor their use to ensure efficient operation, to detect misuse and to supply evidence if required, for use in disciplinary or legal proceedings.

By using Company ICT systems users accept that all use may be monitored.

Sign Off

I have read and understand Gateshead Company's ICT Security Policy and agree to abide by it. I understand that violation of any part of the policy may result in disciplinary action being taken against me.