Albyn Group

ICT System Security & Acceptable Use Policy

Authorship, Revision History and Approval

Date	Version	Author	Role	Changes made/approvals given
March 2012	0.1	Robin Nairn	Finance & Albyn Group Director	Template for Policy

Albyn Group – ICT System Security and Acceptable Use Policy

Contents

Albyn Group – ICT System Security and Acceptable Use Policy

Introduction

Albyn Housing Society Limited (AHS) is the leading registered social landlord for the Highlands. With over 2500 properties in management across nearly 70 separate communities, Albyn has an ongoing development programme of affordable homes for rent and sale and is involved in a number of innovative projects in partnership with other key agencies. AHS has a subsidiary to undertake non charitable trading.

This policy is a group policy. All references to Albyn pertain to AHS and any other member of the Group

This document describes the policies for System Security and the “acceptable use” if its systems which have been adopted by Albyn

This policy defines how Albyn staff should use their ICT systems in order to ensure secure and safe access to data in the best interests of both Albyn and themselves.

Albyn Group – ICT System Security and Acceptable Use Policy

1. General

1.1 ICT systems (including external and internal e-mail, faxes and the Internet/Intranet, phones, smart phones etc.) that are provided by Albyn for business purposes. Whilst use for personal and other reasons is permitted, such use should not contravene this policy and must not compromise the data security principles described here. The personal use of the ICT systems should be limited to lunch breaks and before and after the working day, unless specific permission is granted by the line manager

1.2 Albyn regularly monitors the use of these systems. Misuse will be dealt with under the disciplinary procedure and may in some cases lead to dismissal.

1.3 Albyn staff should consult the Finance and Corporate Manager and seek guidance on the use of Albyn systems for personal use.

2. Albyn Group Data Security Principles

2.1 Albyn Group data consists of all pertaining to Albyn business activities.

2.2 Albyn Group data is held on the servers in the Invergordon and Inverness Offices - Server Rooms.

2.3 All of Albyn Group data is backed up overnight onto an industry standard backup tape(s). In the event of a complete loss of systems, the maximum amount of work that would be lost would be one day's work.

2.4 Albyn uses an industry standard cycle of daily, weekly and monthly backups, to ensure to ensure that we have multiple copies of Albyn Group data.

2.5 Backup tapes are removed to a secure, off site location daily. Documents and other data held on such tapes can be recovered.

2.6 External email messages can be retrieved via Mimecast for up to 180 days and internal emails may be retrieved for up to a year.

2.7 Albyn users are responsible for the security of documents and other data. This responsibility also applies to all types of storage and storage devices and other removable media and information held on phones and smart phones.

3. Data Protection

3.1 Albyn complies with regulations under the Data Protection Act 1984, as amended by the Data Protection Act 1998.

3.2 It is Albyn's policy to protect and hold safe all Personal Information which it requires or needs to possess in the performance and management of its operation.

3.3 In no case will personal information be passed on to individuals outside Albyn without the permission of the individual unless required by law.

3.4 In the event that a third party requests this information, their details are taken and the employee is asked to contact the requester.

The Data Protection Policy and statements are available on the Intranet

4. Email Use and Security

4.1 Due to the nature of the Internet, it is not possible to guarantee delivery, time of receipt or that a third party cannot intercept the message.

4.2 An important communication should always be backed up by an alternative method of communication (e.g. letter or fax). A copy of both messages should be retained on file.

4.3 A disclaimer will automatically be attached to external messages (See Appendix I).

4.4 A commercially sensitive communication should not be sent without the consent of the employee's manager. When authorising a communication, the manager must take into consideration the implication of the external message being read by somebody other than the intended recipient.

4.5 As it is easy to address a message to the wrong person, the employee should always double check that they have the correct addressee before transmitting the message.

The E Mail Use Policy and statements are available on the Intranet

5. Physical security of Server Room in Invergordon and Inverness

5.1 The Server Room at Invergordon contains the systems which maintain and secure all of the Albyn Group Data referred to in this document, including documents, email messages and other files.

5.2 Access to this room is restricted to members of the ICT Team and designated members of the Albyn management team.

6. Use of Albyn Group Laptops

6.1 Albyn Group laptops may be used to connect to the Albyn network, from a home, office or mobile location.

6.2 When out of the office, users of such laptops must use the recommended method of connection, via the secure VPN connections and Remote Desktop Protocol

6.3 Access to Albyn Group laptops is protected by an individual user logon. Users of Albyn Group Laptops must maintain the confidentiality of such passwords and must not divulge them to third parties under any circumstances.

6.4 Data held on Albyn Group laptops is not encrypted. Users should be aware of this and ensure that business confidential information held on such laptops may be at risk if the laptops are lost or stolen.

6.5 It is accepted use of an Albyn Group laptop to hold copies of files and documents which are required for meetings, presentations and for working whilst away from the office. However, it is recommended that staff should delete such files after use, after copying any updated files onto the Albyn network.

6.6 Files, data and documents held on an Albyn Group laptop are not backed up, unless copied to an Albyn network drive.

6.7 Users are responsible for the care of their allocated laptop. Any loss or theft of a computer or data storage device must be reported immediately to the Finance & Corporate Manager who will take the appropriate action to safeguard the security of the information if possible.

7. Use of Home & Personal Computers

7.1 The use of home or other personal computers to access the Albyn's network etc requires to be organised by ICT staff. Permissions will be reviewed regularly by the Finance and Albyn Group Manager.

7.2 The same general principles of information security as defined for Albyn Group Laptops applies to the use of such systems. Confidential data should not be maintained on such system except when required for business purposes.

7.3 Files, data and documents held on a home or personal computer are not backed up, unless copied to an Albyn network drive.

8. Use of Storage Devices & Memory Sticks

8.1 Albyn employees may use the C: drive of their local system (a desktop or laptop) to store files from time to time. Such local storage may be used to support flexible modes of working e.g. to provide a means of transferring documents between home/personal and Albyn systems.

8.2 Employees must recognise that documents/data stored on such devices is not included within the Albyn Group data security and backup procedures, which are limited to the central server only.

8.3 It is recommended that business relevant data and documents are copied to the network at the earliest opportunity.

8.4 Staff who choose to use their C: drive or a memory stick to hold their files must take responsibility for the backup and security of such files.

9. Access for Guests and Visitors

9.1 The access codes for this network will be provided on a visit by visit basis by the ICT staff as appropriate.

10. Misuse of Systems

10.1 Albyn has a duty to ensure that its employees do not receive or send offensive material. No defamatory, libellous, offensive or obscene material may be transmitted or included in any messages. Such misuse will be dealt with under the Disciplinary Procedure.

10.2 Should an employee receive either defamatory, offensive or obscene material, whether via internal or external email, they should inform the Finance Manager or the ICT Officer immediately who will take appropriate action.

11. Internet Access

11.1 Internet access is provided to employees for legitimate business use. Employees are prohibited from accessing websites which are not relevant to the purpose of their employment.

11.2 It is a potential disciplinary offence to access non-relevant websites. This may include:

- pornographic websites
- sites whose use may contravene racial or gender equality legislation
- sites which promote incitement to racial hatred.

Accessing such sites from Albyn systems may lead to the dismissal of the employee.

11.3 Albyn has installed software to monitor employee access to the Internet.

11.4 If staff members are using the Albyn facilities to access websites as part of the personal use permitted under 1.1, the list of sites under 11.2 are prohibited.

12. Telephones

12.1 Telephones are provided for business purposes only. While it is accepted that some personal use may be necessary, such use must be kept to a minimum level.

12.2 Overseas personal calls or calls to premium rate lines are only permitted when required to meet business purposes. Albyn monitors the use of telephones and misuse will be dealt with in accordance with the Disciplinary Procedure.

13. Mobile Phones including personal phones (including smart phones etc.)

13.1 Mobile phones and other similar devices are provided for business purposes only. While it is accepted that some personal use may be necessary, such use must be kept to a minimum level.

13.2 It is accepted that employees may have personal mobile phones in the workplace, but use of them during business hours should be kept to a minimum.

13.3 Theft of such devices is widespread. Employees should take care not to leave mobile phones etc. unattended or in vehicles. In the event of an Albyn device being stolen the employee should report this to the ICT team immediately.

13.4 It is an offence to operate a mobile phone etc. handset whilst driving. The Company instructs that all mobiles, including those fitted with hands free kits, are not used whilst the employee is driving.

14. Incident Management

14.1 An Information Security Incident is any event that results in: the potential or actual loss; the unauthorised access of; corruption of; or communication of information owned by Albyn or held by Albyn on behalf of its customer or partner organisations.

14.2 Information security incidents frequently (but not exclusively) arise from:

a. Abuse (Internet, E-mail, Viruses, Malicious Activity, Sharing Passwords).

b. Access (Unauthorised access to company locations, systems or information).

c. Loss or theft (Loss or the theft of information stored on media or in documents or held on company systems, laptops and other mobile devices).

d. Non-compliance with company policies or guidelines.

e. Any observed or suspected security weaknesses.

14.3 Reporting

All information on security incidents must be reported as quickly as possible through the following channels:

a. The Help-Desk if relating to Customer Support Services or Systems (e.g. break fix or managed services).

b. The Finance & Corporate Services Director or Manager if relating to internal services or systems.

14.4 The Finance & Corporate Services Director maintains an Incident Log of all information on security incidents reported and provides feedback to the individual who raised the incident.

14.5 Incidents will be reviewed locally in a timely manner, prioritised and escalated as necessary and corrective and preventative actions taken. Every six months, summary reports of the information security incident log are presented for review at the Executive Team meetings.

.

Appendix 1

Social Media Procedure

In the workplace

1. Employees must not access social networking sites/the corporate social networking site during working hours unless related to Albyn Business and authorised to do so. Access using Albyn's ICT systems is restricted to lunch breaks and before and after the working day, unless specific permission is granted by your line manager.
2. Employees may not use Albyn's corporate social networking site for personal blogs.
3. Employees must make it clear when posting information or comments on the corporate social networking site that any personal views which are expressed do not represent those of Albyn.
4. Employees must not post information on a social networking site which is confidential to Albyn, its suppliers or customers.
5. Employees must refrain from making reference on a social networking site to Albyn, its employees, its customers and its suppliers.
6. Employees must not post entries on the corporate social networking site/a social networking site which are derogatory, defamatory, discriminatory or offensive in any way, or which could bring the Albyn into disrepute.
7. Employees should be aware that blogs may create documents which the courts can order to be disclosed for use in litigation. Consequently, employees will be assumed to have written any contentious items unless they can prove definitively that they have not done so.
8. Albyn will monitor its IT systems as is deemed necessary in order to prevent inappropriate usage. Hard copies of blog entries could be used in any disciplinary proceedings.

Outside the workplace

1. Employees must not make reference to Albyn, its customers or its employees on social networking sites.
2. Offensive, defamatory or inappropriate comments about Albyn, its customers, suppliers or any of its employees that employees write on social networking sites will not be tolerated.
3. Employees must not make discriminatory or offensive comments about work colleagues on social networking sites.
4. Employees must not divulge confidential information about, or belonging to Albyn, its customers or suppliers on social networking sites.

The above principles apply equally to information or comments posted by employees from their home (or other personal) computers and irrespective of whether the posts are done during working hours or in the employee's own personal time.

Disciplinary action

1. Employees whose conduct breaches this policy in any way will be subject to disciplinary action in accordance with Albyn's disciplinary procedure up to, and including, dismissal.

2. Any blog entries made inside or outside the workplace that are defamatory, derogatory, or discriminatory about the Albyn, its customers, suppliers or employees will be investigated as gross misconduct. If substantiated, such conduct may lead to summary dismissal after the due process of Albyn's disciplinary procedure has been followed.

Appendix 2

The following will act as guidelines when considering if the use of ICT is acceptable or unacceptable.

1. Acceptable Use

1.1 The following criteria will be used to assess whether usage is acceptable:

- Be in support of business and service needs consistent with service and Albyn policies
- Be in support of an individual's approved duties
- Be consistent with the regulations appropriate to any system or network being used / accessed
- Adheres to policies which reflect protective marking of data and safeguarding of protected data
- May be for limited personal usage provided this is not associated with monetary reward, is undertaken in the user's own time (non work hours e.g. lunchtimes, before or after work) is not interfering with the delivery of Albyn's services, does not violate this or any Albyn policy and is a lawful activity

1.2 Any questions or guidance about the levels of acceptable usage should be discussed with the individual's line manager or as indicated in the policy

2. Unacceptable Use

2.1 It is unacceptable for a user to use, submit, publish, display, download or transmit on or from the network or on any Albyn ICT system or device which connects to Albyn's network or is operated by the Albyn any information which:

- Restricts or inhibits other users from using the system or impairs the efficiency of the computer system;
- Violates or infringes upon the rights of any other person, including the right of privacy;
- Is contrary to the Albyn's harassment policy and procedures;
- Contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material;
- Encourages the use of controlled substances or the use of the system with criminal intent; or
- Uses the system for another illegal purpose;
- Breaches legislation or statutory requirements which Albyn has to comply with e.g. Data Protection Act

2.2 It is unacceptable for a user to use these facilities and capabilities of the systems to:

- Conduct any non-approved business;
- Download unapproved software;
- Undertake any activities detrimental to the reputation of Albyn;
- Transmit material information, or software in violation of any local, national or international Law;
- Undertake ,plan or encourage any illegal purpose;
- Deliberately contribute to websites that advocate illegal activity;
- Harass an individual or group of individuals;
- Make offensive or derogatory remarks about staff on interactive life style websites;
- Post offensive, obscene or derogatory photographic images, commentary or soundtracks on interactive life style websites;
- Transmit or produce material which breaches confidentiality undertakings;
- View, transmit, copy, download or produce material including (but not exhaustively) software, films, television programmes, music, electronic documents, and books which infringe the copyright of another person or organisation;
- Conduct any unauthorised political activity;
- Conduct any non-Albyn related fund-raising or non-Albyn related public relations activities;
- Access or transmit information via the internet, including email in an attempt to impersonate another individual;
- Attempt to gain deliberate access to facilities or services which you are unauthorised to access;
- Deliberately undertake activities that corrupt or destroy other users' data, distribute the work of other users or deny network resources to them ,violate the privacy of other users, waste staff effort or networked resources;
- Make any unauthorised purchases;
- Send personal, sensitive, confidential data by email to external contacts unless it is identified by both the sender and receiver of the email having secure email addresses.

Clarification of any of the above acceptable and unacceptable uses should be sought from your line manager or as indicated in the policy

Should users indulge in unacceptable use as defined above they may be subject to disciplinary action under the relevant disciplinary procedures. In certain cases this may amount to gross misconduct e.g. accessing pornographic or obscene material which would normally lead to summary dismissal, subject to normal disciplinary procedures.

Appendix 3

Albyn Group Email Disclaimer

The following sample disclaimer will be appended to all emails sent vie the Albyn mail server. Variations of the disclaimer are in use which takes account of the office location and Albyn Enterprise Staff

INVERGORDON DISCLAIMER

Staff Name
Job Title

Albyn Housing Society Ltd
98-100 High Street
Invergordon
Ross-shire
IV18 0DL

A Scottish Charity - No: SC027123

Phone: 01349 ??????
Mobile: 0???? ??? ???
Fax: 01349 853 859
Email: firstname.surname@albynhousing.org.uk
Web: www.albynhousing.org.uk

The information contained in this communication from firstname.surname@albynhousing.org.uk sent on **Auto Date** at **Auto Time** is intended solely for use by intendedrecipient@intendedrecipeint.??? and others authorized to receive it. If you are not the intended recipient, employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication and its attachments is strictly prohibited.

Any views or opinions expressed in this email by **Staff Name** are not necessarily those of Albyn Housing Society Ltd.

Albyn Housing Society Ltd may monitor email traffic data.

Although this email has been scanned for viruses and malicious content, for your own protection you should ensure that the email is checked by your own up to date virus scanner.

APPENDIX 4

ICT SYSTEM SECURITY & ACCEPTABLE USE POLICY

RESPONSE FROM ROBIN NAIRN TO QUESTIONS RAISED PRIOR TO STAFF CONSULTATIVE FORUM MEETING ON 13 MARCH 2012

General Comment

The policy that we are seeking approval for is based on policies that are adopted by other companies and are based on best practice guidance from Croners etc. On that basis the information contained below attempts to answer the questions raised.

Feedback for SCF from Non GMB Group.
ICT System Security and Acceptable Use Policy:
10. Misuse of System.
10.1 It was acknowledged by the group that people may have individual interpretations of the words 'obscene' and 'offensive'. Perhaps some examples could be provided?

The government issued legislation about a year ago that basically said the definition of obscene and offensive language and behaviour is defined by the person who it is aimed at or comes into contact with it, not the individual who initialises the behaviour or action. We are therefore unwilling to try and give a list and leave it to individuals to make their own judgements based on the details given in this section.

10.2 The group feels that there could be an intermediate stage before reporting the receipt of this type of material to the Finance Manager or ICT Officer. For example, where 'funnies' have been circulated and accepted previously, it would be more appropriate for the person who receives them to contact the sender as a first step and request that this type of material is no longer acceptable rather than escalating straight to a formal report.

We would hope that staff would deal with these matters on an informal basis; we are attempting to ensure that staff in receipt of what they consider to be offensive or obscene have a formal procedure if necessary

11. Internet Access:
11.1 This paragraph needs to be cross referenced to paragraph 11.4. It was suggested that the paragraphs in this part of the policy are re-ordered to make it clearer at first reading.

We do not feel that it implies that you cannot state that you work for Albyn. If you feel that it does imply this can we work on the wording to avoid this implication at the meeting?

We understand that this relates to personal Facebook sites etc. Any employee under the terms and conditions of employment has a duty to act reasonably in representing Albyn at all times. It is not the intention of Albyn to stop staff making comment such as those illustrated above but that if these comments undermine the organisational goals and aims Albyn has the ability to question and if appropriate take disciplinary action.

The other point we would like staff to be aware of is that these types of comments on Facebook etc. is that they will be a record of the remark forever and is available worldwide whereas verbally making these remarks is to a specific audience and, therefore, potentially less damaging.

Appendix 1. Social Media
General comments from the group:
Access to the Facebook page. Staff are not clear from this paper how the Corporate Facebook page is going to work and when and if staff from different departments will need to check it in order to respond to comments left etc. A general statement would be appreciated.
A group of staff from all departments will be responsible for responding to comments. Any comments made by anyone will be checked by the Corporate Department prior to publication on Facebook and therefore might be removed etc. as outlined in an answer to a question below.

Should staff be posting anything on the Corporate Facebook site at all?
In response to comments as outlined above

The group would like to clarify whether or not they can still list Albyn as their employer in the personal information part of their page. Also can they still make general statements e.g. "I had a rubbish day at work?"
We do not feel that it implies that you cannot state that you work for Albyn. We would actually encourage staff to be proud of Albyn and that you are the best ambassadors that Albyn could have.

Staff would like to have a little more information on how personal monitoring works.
The software that we are using and have used for a long time is "Webroot". This is a recognised web monitoring and filtering tool used by many company across the globe. It works based on us selecting the "types" of sites that it is felt appropriate to be filtered. This will include the types of sites detailed in 11.2 of the document. Webroot categorises all web sites depending on content and stops access to all these sites. (We are able to release sites that are filtered if appropriate). This filters out many sites that we would all reasonably consider to be offensive. It will not filter out sites that are not business related, so individual members of staff will have access however staff are trusted only to access these outside working hours.
It should be noted that we do not routinely audit staff use but that when we have reason to believe there is a risk of inappropriate use of the web then Albyn is able to use Webroot to verify what activity has taken place

11. Internet Access page 7
Appears to contradict Appendix 1 no. 1 unless 'websites that are not relevant to the purpose of their employment' in 11.1 is defined in 11.2 as 'non-relevant websites' which are restricted to the sort of sites listed in the bullet points below 11.2.

We don't think that this comment goes with the preceding question from staff. We think that we probably need to reiterate that non-work use should be limited to outside work hours and observe the restrictions on using inappropriate sites, etc.

Social Media Procedure Appendix 1 No 5, (In the workplace) and No 1 (Outside the workplace) page 10
This seems to imply that an employee can't disclose that they work for Albyn in their profile on their personal Facebook site. Is this the case?
We do not feel that it implies that you cannot state that you work for Albyn. We would actually encourage staff to be proud of Albyn and that you are the best ambassadors that Albyn could have.

If you feel that it does imply this can we work on the wording to avoid this implication at the meeting?

Does this mean that staff can go onto their own Social Network sites at lunchtime?
Yes it does, provided they observe the rules, etc

Generally
The group felt that staff should have been asked before staff team photographs were posted on the corporate site. Several members objected to their photo being displayed in this way.
The photographs used were those which were taken for the annual report. The annual report is available online, and was circulated to tenants / contractors / consultants. The annual report is also available for anyone at both the Invergordon and Inverness reception. Only the name of the department features as the title of the photograph. No individual names are given.

The group felt that not to be able to say 'had a rotten day at the office' interfered with their freedom of speech.
We understand that this relates to personal Facebook sites etc. Any employee under the terms and conditions of employment has a duty to act reasonably in representing Albyn at all times. It is not the intention of Albyn to stop staff making comment such as those illustrated above but that if these comments undermine the organisational goals and aims Albyn has the ability to question and if appropriate take disciplinary action.
The other point we would like staff to be aware of is that these types of comments on Facebook etc. is that they will be a record of the remark forever and is available worldwide whereas verbally making these remarks is to a specific audience It should be noted that even if your page is available to "Friends Only" your friends could choose to share any comments you make, and you are then dependent on their privacy settings

We believe Roddy has software that can exclude staff access to 'non-relevant' websites.

The software that we are using and have used for a long time is "Webroot". This is a recognised web monitoring and filtering tool used by many company across the globe. It works based on us selecting the "types" of sites that it is felt appropriate should be filtered. This will include the types of sites detailed in 11.2 of the document. Webroot categorises all web sites depending on contents and stops all these sites. We are able to release sites that are filtered if appropriate. These filters out many sites that we would all reasonable consider to be offensive. It will not filter out sites that are not business related, so individual members of staff will have access however staff are trusted only to access these outside working hours

I can't stress too strongly the group's anxiety about the potential for people outside the organisation to post comments which may be derogatory to staff members. Where is the protection for the reputation of individual staff members? Is there any opportunity to monitor and remove these before they are published?

We can confirm that the Corporate Department has have made every effort to ensure that the page is set with security measures and privacy settings so that any comments made by the public are screened before they are published on the page. An email will be sent to the corporate email address informing Carolynn and Lynne of any changes / additions to the page. We will then screen messages prior to publishing them on the 'wall' of the Facebook page. Any references to either staff / tenants / or others in a derogatory way will not be published on the site. However in order to respond to the individual it was agreed within the group that anyone contacting Albyn in this way will be messaged privately informing them of an appropriate way to raise any issues they have. Any complaints will still have to follow the complaints procedure. Individuals can currently comment about Albyn or Albyn staff through social media without our knowledge. By having an official Albyn page we are giving people an opportunity to contact Albyn, where Albyn can respond.

Follow up on photographs etc.

The Society now has procedures that allow staff to authorise the use of their image for Albyn Business (photo video etc.)

APPENDIX 1

SCF MEETING 13 MARCH 2012: MINUTE EXTRACT

3. CONSULTATION PAPERS

3.1 ICT System Security and Acceptable Use Policy

3.1.1 Mr Nairn noted that the vast majority of the Policy had not been commented on by staff and was therefore deemed acceptable. Mr Nairn tabled his answers to the questions that had been raised via the two staff groups and asked that these be attached to the minutes for all staff to see. The Committee were given time to read the tabled document. This document is attached to the minutes as tabled. The Policy will be amended to reflect the outcomes of today's discussion.

Comment see attached

3.1.2 Ms Norris referred to the response regarding what is deemed obscene or offensive. She understood that this referred to verbal comments, rather than websites. However, she noted that the Webroot system blocked most, if not all, of those sites that the Society would deem offensive or obscene. Mrs Simpson believed that the Policy was actually referring to emails rather than websites. Her group had wanted to make the point that there should be the opportunity to deal with these on an informal basis and this was confirmed in the written response from Mr Nairn. Mr Rose suggested that perhaps "circular" emails should not be sent to work email addresses, but if received they should only be viewed outside of working hours. He suggested that these types of emails should be sent instead to private email addresses. There is no expectation of privacy for emails sent to a corporate address. Ms Norris suggested that this is made clear to staff. Ms Norris commented that it was difficult to limit reading these until lunchtime as sometimes the content is not known until opened. She agreed that these types of emails should be sent to private email addresses. Ms Norris suggested that staff are given the opportunity to ask the senders to use their private email address, before the policy is implemented. However, there was concern that the policy would stop the exchange of similar emails between staff internally. It was suggested that this policy should apply to the re-circulation of all these types of emails, as even non-offensive emails took time to read.

Action

An informal approach will be adopted to where the receipt of such material is not able to be controlled by the recipient but staff will try and ensure that action is taken to avoid subsequent incidents

3.1.3 Mr Nairn said that the policy would be flexible and would consider each case. The policy would provide a formal structure for those who needed to report a particularly offensive or obscene email or material. Mrs Simpson was concerned that every member of staff worked hard and deserved to share a joke every now and then. It was agreed that the policy would not be draconian and would allow staff flexibility out of working hours. In addition, any issues related to this, such as a member of staff using their personal Facebook page in working hours, would be a management issue. The comments made by Mr Nairn within the response document were considered reasonable and will be included in the policy.

Action

Noted

3.1.4 It was confirmed that staff are allowed to use their computer during lunch hours, but it was a management issue to ensure staff take appropriate breaks.

3.1.5 There was discussion about the use of staff photos on the Facebook page. Staff had been concerned that their photos had been used. Further information on this subject was due to be provided just as Miss Lawrie was taken ill and therefore some staff were not aware what had been included on the Facebook page until after it went live. It was noted that the staff photos had already been published and were available electronically through the website via the Annual Report, so the images were in effect already available world-wide. In addition, the photos were group ones with no staff named individually. The idea had been to provide the human side of the Society, rather than photos of just bricks and mortar.

Action

Subsequent SCF meeting has agreed an approval mechanism for staff to approve or not the use of personal images

3.1.6 It was agreed that in future when staff photos are taken for the Annual Report and Facebook, staff will need to inform their line manager if they do not wish to participate in the photo process. Mr Nairn expressed his disappointment that some staff thought that providing a human face for Albyn was not important.

Action

Subsequent SCF meeting has agreed an approval mechanism for staff to approve or not the use of personal images

3.1.7 Mrs Simpson referred to the responses regarding staff posting on their Facebook page about where they work and general comments about work, for example, “I had a rubbish day at work today”. Mr Nairn confirmed that staff posting where they worked and making general comments like this is reasonable on an occasional basis. However, if the number of occurrences were high that might have a reputational effect on the Society and would lead to enquiries being made. He also asked staff to bear in mind that they are ambassadors for Albyn and that any comments made will continue to exist in writing. The policy would only address serious, detrimental comments about Albyn or members of staff. Mr Rose commented that posting a comment such as "I had a bad day at work" might lead a friend on Facebook to ask why it had been bad, and staff would then have to carefully consider how they respond.

Action

Noted

3.1.8 With the agreed amendments, Mr Nairn proposed that the policy was approved.

3.1.9 The Policy, with the additional wording, was therefore proposed for approval by Mrs McLaughlan and seconded by Mrs Simpson.