INFORMATION TECHNOLOGY

General

1. IT is a critical tool for the achievement of the GL mission and vision, as well as for cost savings and ensuring maximum efficiency. There are various technical IT procedures covered in detail in the IT manual including passwords and access codes. What follows is GL's IT policy.

2. Failure to adhere to the provisions of this policy may result in the suspension or loss of access to GL resources.

3. Should an individual's access be suspended, GL shall inform the individual immediately and shall afford the individual an opportunity to respond. GL shall then determine whether some alternative course of action, is warranted and shall follow the procedures established for such cases.

4. Any IT-related service calls that are not of a routine maintenance nature shall be authorised by the Finance and IT Coordinator.

5. GL can contract IT companies for the provision of IT and related services.

Equipment and software

Use

6. GL may issue equipment to members of staff requiring these for their work.

7. All GL office equipment shall be used for GL business.

8. All staff in possession of GL equipment must sign a form taking responsibility for the equipment **(Form FN08: GL equipment form).** Damage to and loss of equipment due to negligence of a staff member shall require the staff member to replace or pay GL the value of the laptop.

9. Staff are responsible for taking due care of GL equipment including:
   - Insuring that these are ALWAYS carried as hand luggage on aeroplanes.
   - Stored safely.
   - Have valid anti virus software that is regularly updated and runs regular
   - checks.
   - Never left unattended.

10. GL reserves the right to recover any costs or losses that may result from negligence in the care and security of office equipment.

11. Equipment owned by GL shall under no circumstances be taken away from the office at any time for use other than for GL designated work and events.

12. Office equipment and software shall be signed out by the office manager and returned accordingly.

13. Office equipment and software shall be locked at all times. It is the responsibility of the ITO to ensure that this is done and to keep the key in a safe place.

Ownership and insurance

14. The following conditions apply:
    - GL is not in a position to insure self-owned lap tops because the premium on such is extremely high and may exceed the replacement value.
    - Staff using their personal or company owned laptops on GL premises are expected to exercise maximum caution including using the security cord; never leaving laptops on their desks at the end of the day or at weekends when they are away from the office; and locking their laptops away in cupboards to which they keep the keys when they are out of the office for extended periods.
    - In the event that a self owned laptop is stolen from the GL premises or on GL business even after all the above have been observed and in the assessment of the CEO the loss is not the fault of the staff member concerned GL will replace the laptop to a maximum amount of the market value of the laptop at the time of its being stolen.
    - GL bears no responsibility for a self-owned laptop that is stolen away from the office premises.
    - As important, if not more important than the laptop itself, is the data contained that often represents an invaluable amount of time and work paid for by GL. Therefore a critical condition of any laptop use (and part of the loan agreement) shall be that the staff member concerned backs up their data weekly on the H drive and that all information that should be made available on the Public drive is also saved there weekly. GL takes responsibility for the further back up of data from the server.

Loans for laptops

15. All staff are entitled to a desk top computer. Should staff wish to work off laptops they will be provided with soft loans to purchase their own laptops.

16. Staff who opt to buy their own laptops shall be availed loans to do so and they shall sign a loan agreement form. Should a staff member resign before the loan has been fully paid this will be deducted from any amounts owing to the staff member.

Care and maintenance

17. Copying of large personal files (especially audio visual files) onto GL computers is prohibited.

18. Eating and drinking in close proximity to computers is not allowed at any time.

19. Connection of personal equipment to the GL network without permission from the ITO is prohibited.

20. Copying or removing software from GL equipment is prohibited.

21. Computers must be switched off after use. In the case of the GMDC lab, the station must be left ready for the next patron. Leave the monitor on the login screen, pick up all your papers and push in your chair.

22. It is the responsibility of all staff to ensure that their computers and laptops have the latest anti virus installed.

23. It is the responsibility of all staff to ensure that the anti virus is programmed to run a full system scan every week.

24. The ITO shall be responsible for ensuring routine maintenance of equipment including virus checks.

25. All staff shall be provided with equipment cleaning fluid and shall be expected to keep their equipment free of dust at all times.

Protection of Intellectual Property

26. GL has the responsibility to uphold software license provisions and copyright laws for the software that is officially installed and the publications officially posted on the Organization network. The organisation cannot accept responsibility for unofficial software installations, publication postings, and messages that are the acts of private individuals acting in a private capacity. The organisation will, however, remove software or publications from its network and computing facilities whenever it discovers their installation constitutes copyright violation, piracy, or other form of malfeasance.

27. GL information available via the website is copy righted to the organisation.

28. Permission must be sought from the CEO for usage of the GL materials. GL must be acknowledged by the user when the material is being used.

Email, Internet and Virtual Private Network

Authorised access and use

29. Only GL staff members are allowed to use the computers that are linked to the domain. The ITO may authorize access to the GMDC computers.

30. All staff members shall be supplied with E Mail addresses; shall be required to be conversant with its use and with use of the Internet; shall be required to run weekly virus checks on their computers and report any dysfunctional computers to the ITO when necessary.

31. All staff members at a senior level shall be required to make appropriate arrangements to be able to access their E Mail remotely, that is away from the office. Staff should explore new and affordable technologies such the satellite telephone and Internet connections offered by Neotel and others.

32. Users will not use another person's computer account without permission. Passwords will be kept private and users will not allow unauthorized use of their accounts.

33. GL computing infrastructure and facilities are for GL purposes only; these purposes include administrative, instructional, and professional activities (e.g., research) integral to the mission of the organisation.

34. Use of the Internet at the office for any purpose other than work related is strictly prohibited. In particular surfing of the Internet for pornography is forbidden and constitutes a grave disciplinary offence. Should a supervisor or the CEO/DP have any cause to believe that the Internet is being abused, he or she is entitled to obtain information on how particular staff members are using the Internet from the ITO and to take action accordingly.

35. GL computing facilities and networks cannot be used for personal business or compensated outside work, or for the benefit of organizations not related to GL except in connection with scholarly pursuits (e.g. organization publishing activities), consulting activities, and services that do not violate GL or GL policies or State regulations and laws.

36. The origination of "junk mail," chain letters, or otherwise flooding the network with huge volumes of unsolicited electronic mail is not appropriate use of network resources and will not be tolerated. GL reserves the right to permanently block unwanted mail.

37. GL shall monitor Internet usage on a monthly basis per user, and shall raise any excessive or inappropriate use of the Internet with users in accordance with rules set out here, and take disciplinary action as appropriate. GL reserves the right to charge for excessive inappropriate use of the internet that has no relation to the work of the organisation during working hours. GL further reserves the right to block websites that are purely of an entertainment nature or that contradict the values of the organization that feature in the 100 most visited websites in the monthly statistics.

38. GL reserves the right to block use of certain Internet websites that have no relevance to its work and which records show are being excessively visited by staff against the principles of the organization, or to the detriment of time management. Examples are pornography sites and face book.

39. Information stored on the GL server is deemed to be private and confidential. Access to the server via the VPN is given to all GL staff. Logins and passwords are confidential and cannot be shared with anyone outside the organisation. Anyone who is found to be in breach of this condition will be subject to GL's disciplinary procedure.

Harassment

40. All users have the right to freedom from harassment and undesired information by computer or network usage by others.

41. No user may use GL facilities to harass any other person. The following shall constitute computer harassment:
    - Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend, or bother another person by conveying obscene language, pictures, or other materials or threats of bodily hard to the recipient or the recipient's immediate family;
    - Intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;

- Intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate;
- Intentionally using the computer to disrupt or damage the academic, research, administrative, institutional or related pursuits of another;
- Intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

Privacy and confidentiality of records and communications

42. GL shall take all reasonable precautions to protect the privacy and confidentiality of organisational matters and communications. The organisation will not seek access to user documents or messages except where necessary to:

- Meet the requirements of GL Policies and Regulations.
- Protect the integrity of the organisation's information technology resources, and the rights and other property of the organization;
- Allow system administrators to perform routine maintenance and operations, and to respond to emergency situations; or,
- Protect the rights of individuals working in collaborative situations where
- Information and files are shared.

E mail etiquette

43. E Mails using GL - provided E Mail addresses shall carry a short specific header regarding the content of the E Mail: EG Invitation to launch of study on gender and local government 22 March @18.00.

44. All E Mails shall carry the name, designation, organisation name, address, phone and fax number, GL website and logo, face book, twitter and skype addresses of the staff member as demonstrated in the template below.

Staff member name and surname
Designation
Gender Links
9 Derrick Avenue
Cyrildene, Johannesburg
South Africa 2198
Phone: + 27 (0) 11 622 2877
Fax: + 27 (0) 11 622 4732
Skype:

www.genderlinks.org.za
Facebook www.facebook.com/GenderLinks
Twitter: @Genderlinks

45. All E Mails shall be brief, polite, and to the point.

46. Staff shall acknowledge all E Mails from a supervisor or CEO/DP especially when these concern action to be taken and indicate what action has been taken or is planned.

47. In copying E Mails to multiple recipients staff shall be mindful of striking a balance between keeping all relevant parties informed and avoiding information overload, especially for senior staff within and outside the organisation.

48. Staff shall endeavour to take action on E Mail of a general nature before forwarding this to more senior staff, especially with respect to E Mails addressed to the CEO.

49. Staff shall be especially mindful of information overload when those to whom E Mails are being sent are travelling. For example rather than sending or forwarding several E Mails one E mail could be sent at the end of each day with a summary of key queries/information.

50. The size of attachments shall be kept to a minimum through compacting and down sizing techniques and shall generally be less 4 MB.

51. Individual E Mail shall be regularly cleared of old files, especially those that have a large volume.

52. All staff shall acquaint themselves with procedures for and be able to work offsite, using the cheapest possible connection (wireless, 3G etc).

53. All staff working from home shall be accessible on email.

54. All staff shall regularly evaluate their email etiquette against the email etiquette checklist attached as **(Annex K)**.

P drive

55. The P drive is the public drive on which all public documentation and reports are stored. This enables all staff to have access to any of the programme work, institutional information, administrative information etc.

56. The P drive is overseen on a day to day basis by the Executive Assistant.

57. In conformity with the confidentiality clause personal staff records shall be kept separately on the R drive with password access only to the CEO, DFC and HRA.

58. All files saved shall carry file name and date e.g. Opguidelines_0307.

59. Any final document shall carry the word final e.g. Coalfacefinal_0307 and only the CEO is authorised to use the word final in naming files.

60. All articles shall carry the initials of the author e.g. NAPwelcomed_LJN_0307.

61. It is the responsibility of the CEO/DP and of staff to save any information that relates to the organisation on the P drive in its final form, and in the appropriate folder/sub folder. The files are:-

- Finance – includes all of the financial info i.e. financial statements, donor
- information etc.
- Communications
- GL Governance – includes Board info, communications, operational guidelines, and legal

- Institutional – includes all includes all administration forms, Staff members next of kin info, Satellite offices, Well being programme information and physical resources etc.
- GL services
- Monitoring and evaluation – includes the Bi-weekly reports and planners, DFID M and E workshop information, GL evaluation, Institutional M and E, Monthly institutional reports and Programmes M and E
- Partners – includes information on GL's partners
- Programmes – includes all of the programmes work done by GL
- Resources – includes all of the publications produced by GL
- Strategic planning – includes all GL 3 years, annual and trimester strategies.
- Website/IT – includes information relating to the website and IT

Photo library

62. This is where all of GL's electronic photos are stored.

63. The Communications Programme officer shall generate a photo library systems report at the end of each month detailing the number of uploads done, indicating the themes classified and country of the photographs.

64. A first edit of photos shall take place on the camera, and thereafter on the computer, to reduce the number of images saved on the P drive that cannot be used.

65. All photos saved shall have a file name with name or description of photo, country, photographer's initials, date e.g. RoseTamae_SA_clm_220307.

66. Photos shall be saved at the back end of the website using a software on which all staff will be trained.

67. Designated photos shall be made accessible to the public for sale through the website.

68. Topic files used in the photo library shall be the same as those used in the VRC and the Opinion and Commentary Service.

69. All photos saved to the photo library shall be captioned, assigned key words, and carry the name of the photographer.

Backup

70. All data shall be stored on GL systems to enable backup.

71. Data backup is done on a daily, weekly and monthly basis.

72. The Data Back up tapes are stored at a location away from the office premises.

73. Each week the hard disks are swapped.

74. As an additional precaution, staff are required to backup their files on the C or hard drive of their office computer and on the H drives, the drive on the server for individual back up.

Contacts database

75. GL programme staff shall be responsible for administering the GMDC registration form at all functions so as to capture the information needed for this database. Staff are also responsible for compiling a composite form for workshop reports and may seek the assistance of the Housekeeper or Receptionist in doing so.

76. The GMDC forms shall be uploaded using an online form upon completion of workshops for entry into the database. Those contacts that agree to be public shall be openly available on this website. Contacts that do not wish to be available through websites shall be available to GL only through the back end of the website.

77. If any staff member should become aware of information about a contact being out of date, this should be drawn immediately to the attention of the Executive Assistant, who will be solely responsible for the updating of the GMDC.

78. The Executive Assistant (EA) shall be responsible for adding new contacts to the list serve after each major event. The EA shall generate a contacts database systems report detailing the number of updates made on a monthly basis.

List serves

79. GL has a general GL list serve that includes most names on the database (except where persons may have asked to be unsubscribed).

80. All new participants in GL events shall be automatically added to the list serve and data base but removed if they ask to unsubscribe.

81. This list is used to send out information of a general nature, such as job announcements; press releases; publication announcements; sending out the Gender Justice Barometer (GJB) as well as announcing new articles on the VRC and the Opinion and Commentary Service.

82. Each message shall carry a concise heading. Attachments and heavy files shall be avoided.

83. The GL list serve shall be used selectively to ensure that only information of interest to the recipients is sent out and that not more than one or two messages are sent out each week.

84. The main operators of the list serve shall be the EA, Communications manager, and the website consultant who is in charge of sending out newsletters. The CEO/DP shall monitor usage of the list serve closely and shall limit its usage where necessary.

85. All GL Generals must be approved by the CEO/DP before they go out and checked for Email header, appropriate links, specific dates, times and contact information.

Website

86. The website is organised according to GL's POA. Any new information, publication and reports shall be loaded onto the website. The rules governing all of the processes and the admin pages can be found in the complete IT manual.

87. The website shall be updated on a weekly basis and shall be current at all times. Individual programme officers shall be responsible for ensuring that new information generated is placed on the website. The DP with the ITO and appropriate IT support shall ensure that this is done. The HRA shall ensure that the GL staff page is maintained and kept up to date at all times.

88. The Communications department shall furnish the CEO/DP with a monthly report quoting statistics on usage of the website with recommendations for improving content, usage and outreach. The CEO/DP shall review this report and conduct a monthly review of the website and all IT matters that shall be discussed at a monthly programme review meeting. The CEO/DP may, in addition, at any time if the course of the month conduct spot checks to ensure that proper systems are being adhered to and that regular updates are being made.

Virtual Resource Centre (VRC)

89. The VRC is a special tool for trainers that contains case studies, trainers notes and cross references to training material.

90. The responsible programme staff shall update the VRC on a weekly basis with at least ten new relevant case studies per month.

91. All VRC and case studies have to be approved by the DP before they are published.

The GEM Opinion and Commentary Service

92. This consists of articles that are commissioned monthly and distributed via E Mail as well as stored on the website via date, theme and author.

93. The day to day management of the website storage of this resource is the responsibility of the Communications department under the overall direction of the DP.

E-conferencing

94. The GL website has a permanent cyber dialogues or E conferencing facility under the social networking platform.

95. This website shall be used for training, online seminars, network meetings and any other e-conferences as may help to leverage the work of GL; IT capacity among GL partners and to save travel costs.

96. E conferences shall be configured in a way that the countries and sex of participants can be identified. The Communications department shall be responsible for compiling such data and including it in the monthly IT report.

97. All e-conferences shall be summarised by the appropriate staff member and these records posted to the appropriate programme area.