

Confidentiality

Employee Relations

Contents

Overview	3
Audience	3
Responsibilities	3
Policy.....	3
Guidance.....	3
Staff files	3
General access.....	3
Limited access	4
Preserving confidentiality	4
Breaches of confidentiality	5
Further information for UK-appointed staff.....	5
File location	5
Personnel Information Management System (PIMMS)	5
Home address, phone number and next-of-kin	5
Medical information	5
Sickness absence information.....	5

Overview

This section defines the British Council policy towards confidentiality. It covers:

- staff files
- Personnel Information Management System (PIMMS)
- medical information
- sickness absence information
- preserving confidentiality
- breaches of confidentiality.

Audience

This guidance applies to all British Council staff.

Responsibilities

All members of staff are responsible for adhering to the policy and guidance defined in this section.

Policy

The British Council keeps a certain amount of confidential information about its staff. Generally, this consists of:

- staff files
- personnel information held electronically
- sickness absence information.

All such information relating to an individual member of staff remains confidential, except where it is included in external British Council media, such as the British Council's Annual report or internet site.

Guidance

Staff files

A file is kept on each member of staff. Its contents normally include:

- application form and references originally submitted to the British Council
- medical questionnaire
- record of the recruitment process
- seven most recent performance evaluations
- most recent printouts from personnel system (if applicable) - personal details, academic background, postings and employment history, and so on
- other correspondence (for example, letter of appointment, subsequent postings, details relating to unpaid leave, and so on)
- records of any formal appeals and disciplinary procedures
- references for current or former staff applying for posts outside the British Council.

This list is not exhaustive.

General access

The following have access to staff files, if they need to for specific operational purposes:

- Director General
- HR staff
- Country Directors, in their own offices, and equivalent senior managers
- Legal Adviser
- data protection officer.

In addition, individual members of staff have access to their own records.

Limited access

Recruiting managers and line managers have limited access:

- Recruiting managers can see the three most recent performance evaluations for applicants for jobs.
- Line managers can see copies of performance evaluations on staff they manage, in certain circumstances. There must be a demonstrable operational reason to check the formal record for additional information on a member of staff's achievements, experience and development, for example, where the line manager:
 - is newly-appointed, and needs to find out more before agreeing a new development plan and/or job plan
 - is considering redefining the duties of the job, and needs evidence of relevant experience.

In these cases, a manager would normally only need to read the three most recent performance evaluations. Seeking access to such information must form part of an open discussion with the member of staff about relevant issues, and must not be seen as an alternative to discussion.

Line managers looking at previous performance evaluations for purposes other than recruiting:

- must inform the member of staff and say why the information is needed
- must not allow the information to influence the content of current or future performance evaluations
- must not use the information in any action being taken in respect of a new performance problem.

Preserving confidentiality

It is important for managers to maintain confidentiality when they are dealing with matters relating to staff. This:

- protects the reputation of the individual member of staff
- enables members of staff to discuss sensitive issues with their managers with confidence
- helps build a relationship of trust between management and staff
- demonstrates the British Council's integrity as an employer
- ensures conformity with Data Protection legislation.

Managers are entrusted with such confidential information on employees as is required for operational or legal reasons. In line with the Code of Conduct, such information must not be shared with others unless there is a genuine operational or legal 'need-to-know'. If there is any doubt about passing on confidential information, you must refer to the original source or owner of the information.

Managers must take the following steps to preserve confidentiality:

- share verbal or written information on a 'need-to-know' basis only
- avoid e-mailing any confidential information except where absolutely essential (and, in this case, making use of any facility for protecting its confidentiality)
- keep hard copy information secure in a lockable cabinet
- seal confidential correspondence as 'staff-in-confidence'
- shred confidential waste

- store in private storage areas any information held electronically on networked systems.

All personal matters discussed between managers and staff, including referral to advisory or staff assistance services, are regarded as confidential and must not be passed on.

Breaches of confidentiality

Any breach of confidentiality must be investigated. A member of staff who believes there has been a breach of confidence in respect to his or her case may appeal against the person believed to be responsible for the breach. Disciplinary action may be taken against the manager concerned.

Further information for UK-appointed staff

File location

Files for UK-appointed staff are held in HR registries in London and Manchester. Staff files or material from them can be read only in HR. Exceptions are made if legally required and for:

- geographical directors who may take copies of evaluations overseas to discuss recruitment with country directors
- recruiting managers in the UK regions or overseas.

If a manager in London needs to see documentation which is normally held in Manchester, the documentation is sent to the HR registry in London for the manager to read there, and vice versa. Confidentiality must be maintained at all times.

Personnel Information Management System (PIMMS)

PIMMS stores information on UK-appointed staff and harmonised staff:

- home addresses, phone numbers and next-of-kin details
- other information, for example, personal details such as date of birth and education.

For more detailed information about what's in PIMMS, see the PIMMS guide online.

Staff have the right to see their personal details kept on PIMMS. Access to the system is restricted to staff in HR.

Home address, phone number and next-of-kin

This information is available only to:

- HR staff
- emergency officers.

Exceptionally, the address or telephone number is disclosed if a line manager needs to contact a member of staff urgently. This information is not released to friends (even within the British Council) or external enquirers. The HR registries will forward correspondence on request.

Medical information

- HR registry holds medical information relating to staff working in the UK.
- International Assignments Team holds medical information on UK-appointed staff serving overseas.

Sickness absence information

- Sickness absence and associated information on staff in the UK is maintained by IMASS and held on the payroll.

- International Assignments Team holds sickness absence and associated information on UK-appointed staff overseas.
- Line managers can supplement their own records by requesting information about dates and patterns of sickness absence, but cannot obtain the reasons for it unless the individual concerned agrees.

Note: Managers can discuss the reasons for sickness absence with their staff, but members of staff are not compelled to discuss the nature of any illness, and a refusal to do so must not be held against them.