



CONFIDENTIALITY

This Essex County Council Model Policy was originally created in 1994 and this issue was released in:	July 2011
Academy Staff were consulted on this document and it was accepted by the relevant committee on :	
It was ratified by the Board of Directors on :	4 July 2011
This policy will be reviewed on:	Summer Term 2014
This policy will be reviewed by:	Finance, Premises and Personnel Committee

This policy was based on that reference below with amendments

Confidentiality Policy
A Model for Schools

Published by:

Essex County Council Learning Services Directorate
County Hall, Chelmsford
Essex CM2 6WN
England

©Essex County Council Learning Services 1994, revised March 2001

Further copies may be obtained from:
Essex County Council Learning Services
Personnel & Development Service
County Hall, Chelmsford Essex CM2 6WN
England

CONFIDENTIALITY

INTRODUCTION

Working in the Academy environment necessarily means having access, in a variety of ways, to information that must be regarded as confidential.

The Confidentiality Policy outlines:

- the various types of confidential information which exist;
- the potential recipients of information;
- the form confidential information can take;
- individual responsibilities of staff in possession of confidential information;
- the potential problems that can arise and how to deal with them;
- the consequences of revealing confidential information without authority.

This policy applies to all staff employed by the Academy, including temporary, voluntary and agency staff.

Staff should also have regard to relevant aspects of the following policies where these have been adopted by the Board of Directors.

- Code of Conduct.
- Public Information Disclosure Act (Whistleblowers).
- Internet/Email Policy.

and to the requirements of the Data Protection Act and Child Protection Procedures

TYPES OF CONFIDENTIAL INFORMATION

Information that is regarded as confidential can relate to a variety of people, for example:

- pupils;
- parents;
- staff/colleagues;
- Board of Directors;
- job applicants.

And a variety of matters, for example:

- home addresses and telephone numbers;
- conduct and performance;
- performance and development review/performance management;
- health/medical;
- pay and contracts;
- references;
- internal minutes, memos etc;
- confidential budgetary or policy information;
- other personal information.

These lists are by no means exhaustive, but will extend to cover any other information of a sensitive nature relating to employees, pupils and others connected with the Academy and to the work of the Academy itself.

POTENTIAL RECIPIENTS OF INFORMATION

Within the course of daily operation, information related to the business or those connected with it, may be requested by, supplied by, or passed to a range of people. This might include:

- internal colleagues (own teachers, support staff, Board of Directors);
- colleagues in other schools;
- management teams;
- pupils;
- Board of Directors;
- trade unions/professional associations;
- parents;
- partner organisations (LA, DfES, Teachers' Pensions);
- other external organisations;
- the public;
- the press;
- contractors/potential contractors.

Clearly, the sensitivity of the information will be partly dependent upon the recipient/supplier and the manner in which it is transferred.

Particular responsibilities

- If someone requesting information is not known to staff, particularly in the case of telephone calls, his/her identity and the legitimacy of his/her request should be verified by calling them back. A person with genuine reasons for seeking information will never mind this safety measure.
- It is a requirement under the Data Protection Act that action is taken to ensure the validity of any caller even if they state they have a statutory right to the information requested.
- Wherever possible requests for information should be made in writing e.g. employee references.
- The same principle applies when sending E-mails and faxes. Staff should always check that the information is going to the correct person and is marked confidential where appropriate.
- Being known as an employee of the Academy may mean being asked for information, for instance, by parents about a member of staff who is off sick. Although this can be awkward, parents must be informed that employees are unable to discuss confidential Academy matters. Persistent enquiries can be referred to the Principal.
- The Data Protection Act refers to the principle of third party confidentiality. Information relating to, or provided by, a third party should not be released without the written consent of the third party or unless an 'order for disclosure' is made by a court of competent jurisdiction.

Where they are unsure what to do, staff should refer the matter to the Principal or line manager for guidance.

THE FORM CONFIDENTIAL INFORMATION CAN TAKE

Confidential information can take various forms and be held and transmitted in a variety of ways, for example:

- manual records (files);
- computerised records and disks;
- written reports/minutes/agendas/file notes etc;
- letters, memos, messages;
- telephone calls;
- face-to-face;
- fax;
- Email;
- Intranet/internet.

The methods of acquiring information can also vary. Individuals and groups may become aware of confidential information in the following ways:

- access is gained as part of the employee's day to day work;
- information is supplied openly by an external third party;
- employees may inadvertently become aware of information;
- information may be disclosed.

Particular responsibilities

- Employees should be aware that they may have disclosed to them sensitive information in the course of their work or outside. In some circumstances the individual may request that the information remains confidential.
- Staff will also need to be aware that they may be obliged to disclose certain information e.g. relating to child protection issues and should make it clear to the individual either that confidentiality cannot be guaranteed and/or direct them to a more appropriate officer or decline to receive the information.

Employees should use their discretion regarding these matters, should refer to appropriate procedures and, if in doubt, should seek advice from the Principal or line manager.

RESPONSIBILITY OF INDIVIDUALS IN POSSESSION OF SENSITIVE INFORMATION

As a general rule, all information received in the course of employment, no matter how it is received, should be regarded as sensitive and confidential.

While it is often necessary to share such information, in doing so, employees should consider the following key points.

- The nature of the information:
 - how sensitive is the information?
 - how did it come to your attention?
- The appropriate audience:
 - who does the information need to be shared with?
 - for what purpose?
 - who is the information being copied to? Why?
 - does restriction of access need to be passed on to your audience?

- The most appropriate method of communication:
 - verbal;
 - written;
 - fax;
 - Email;
 - in person.

- The potential consequences of inappropriate communication.

It is also an individual employee's responsibility to safeguard sensitive information in their possession.

Particular responsibilities:

- Sensitive information should be kept secure.
 - Filing cabinets should be kept locked when unattended.
 - Sensitive information should not be left on desks or the photocopier/fax/printer.
 - Papers should not be left lying around at home or in the car. If confidential materials or paperwork are taken out of the office, precautions must be taken to ensure they are not accessible to third parties.
 - Appropriate steps should be taken to keep track of files which are on loan or being worked on i.e. a record of the date sent and the recipients name and position.
 - If it is necessary to supply personal files through the external mail, this must be effected by recorded delivery.
 - Copies of faxes and Emails should be stored securely.
 - Steps should be taken to ensure that private/confidential telephone calls/conversations are not overheard.
 - Meetings where sensitive or confidential information is being discussed should be held in a secure environment.
 - Confidential paperwork should be disposed of correctly either by shredding it or using the confidential waste facility.
 - Personal data should not be used for training or demonstration purposes where fictional data can be used.

- Computer data should not be left exposed to others' view when unattended.
 - Screen savers should be used when computers are unattended.
 - Machines should be switched off when leaving the office.

- Computer files should be kept securely.
 - Passwords should be used and these should not be disclosed to colleagues unless absolutely necessary.
 - Sensitive data should not be stored on public folders.
 - Staff should be familiar with the security of Email/internet systems.
 - Computer discs should be wiped clean correctly before being reused.
 - Access to individual's computers should be restricted.
 - Any user IDs and passwords used for the internet should remain confidential.
 - All work carried out on a computer should be stored safely either in a personal directory or onto a floppy disk which should be kept securely.
 - Computer files should be backed up regularly and not solely saved to the hard disk.

- A variety of phrases may be used on correspondence to denote confidentiality. As a general rule:
 - post marked 'personal' or 'for the attention of the addressee only' should only be opened by the addressee personally;
 - post marked 'private' and/or 'confidential' may be opened by those responsible for distributing post within the Academy.
- Confidential mail which is then forwarded internally, should continue to carry a confidential tag.

Particular responsibilities

- Employees should have regard to potential difficulties which may arise as a result of discussions outside work. While it is natural (and indeed can be therapeutic) to talk about work at home or socially, staff should be cautious about discussing specific and sensitive matters and should take steps to ensure that information is not passed on. Staff should be particularly aware that many people will have a direct interest in education and schools and even the closest of friends may inadvertently use information gleaned through casual discussion.
- Personal (e.g. home addresses and telephone numbers) and work-related information (e.g. salary details, medical details) relating to individuals, should be not be disclosed to third parties except where the individual has given their express permission (e.g. where they are key holders) or where this is necessary to the particular work being undertaken, e.g. it is necessary for an individual to be written to.
- Line Managers should comply with the procedures for the storage and sharing of information relating to individuals' Performance Management Appraisal Reviews.
- Personal and case files should not normally be shared with third parties other than line managers and those responsible for writing references. Exceptions may apply in the case of legal proceedings.

Employees should use their discretion in these matters and if in doubt, should seek advice from their Principal.

THE CONSEQUENCES OF REVEALING CONFIDENTIAL INFORMATION WITHOUT AUTHORITY

Staff should ensure that they are familiar with the Confidentiality Policy and related Policies. While there is an expectation that staff will use their professional discretion in applying the Policy, they should always seek advice from the Principal and other line managers where they are unsure.

Staff should be aware that serious breaches of the Policy may result in disciplinary action being taken. The severity of the sanction will be assessed with regard to the potential harm the disclosure will have caused to the individual concerned. Some breaches of confidentiality could be regarded as potential serious or gross misconduct, which could result in dismissal.