

## Policy and Guidance Information

### DATA PROTECTION POLICY

Section 1: Policy Statement

Section 2: Background to the Data Protection Act 1998

Section 3: Definitions (Data Protection Act 1998)

Section 4: Responsibilities under the Data Protection Act

Section 5: Notification

Section 6: Data Protection Principles

Section 7: Data Subject Rights

Section 8: Consent

Section 9: Security of Data

Section 10: Rights of Access to Data

Section 11: Disclosure of Data

Section 12: Retention and Disposal of Data

Section 13: Publication of YMT Data

Section 14: Direct Marketing

Section 15: Use of CCTV

Section 16: Appendices

I: Staff Records Management

II: Disclosure of Company Member Information

III: Telephone Protocol for the Disclosure of Personal Information

IV: Records Retention Schedule

V: Photographs to be used in Publicity/Promotional Material

### Section 1: Policy Statement

YMT is committed to a policy of protecting the rights and privacy of individuals (includes company members, staff and others) in accordance with the Data Protection Act. The Company needs to process certain information about its staff, company members and other individuals it has dealings with for administrative purposes (eg to recruit and pay staff, to administer projects, to record progress, to collect fees, and to comply with legal obligations to funding bodies and government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The policy applies to all staff and members of the company. Any breach of the Data Protection Act 1998 or the YMT Data Protection Policy is considered to be an offence and in that event, YMT disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with the company, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that departments who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

### Section 2: Background to the Data Protection Act 1998

The Data Protection Act 1998 enhances and broadens the scope of the Data Protection Act 1984. Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent.

### Section 3: Definitions (Data Protection Act 1998)

#### Personal Data

Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

#### Sensitive Data

Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.

#### Data Controller

Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

#### Data Subject

Any living individual who is the subject of personal data held by an organisation.

#### Processing

Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data accessing, altering, adding to, merging, deleting data retrieval, consultation or use of data disclosure or otherwise making available of data.

#### Third Party

Any individual/organisation other than the data subject, the data controller (YMT) or its agents.

#### Relevant Filing System

Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Please note that this is the definition of "Relevant Filing System" in the Act. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

### Section 4: Responsibilities under the Data Protection Act

The company as a body corporate is the data controller under the new Act.

The General Manager is responsible for day-to-day data protection matters and for developing specific guidance notes on data protection issues for members of the company.

Compliance with data protection legislation is the responsibility of all members of the company who process personal information.

Members of the company are responsible for ensuring that any personal data supplied to YMT are accurate and up-to-date.

## Section 5: Notification

Notification is the responsibility of the Board of Trustees. Details of the company's notification are published on the Information Commissioner's website. Anyone who is, or intends, processing data for purposes not included in the company's Notification should seek advice from the General Manager.

## Section 6: Data Protection Principles

All processing of personal data must be done in accordance with the eight data protection principles.

1. Personal data shall be processed fairly and lawfully.

Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

2. Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.

Data obtained for specified purposes must not be used for a purpose that differs from those.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.

Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.

4. Personal data shall be accurate and, where necessary, kept up to date.

Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by the company are accurate and up-to-date. Completion of an appropriate registration or application form etc will be taken as an indication that the data contained therein is accurate. Individuals should notify the company of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the company to ensure that any notification regarding change of circumstances is noted and acted upon.

5. Personal data shall be kept only for as long as necessary. (see Section 12 on Retention and Disposal of Data)

6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act. (see Section 7 on Data Subjects Rights)

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against

accidental loss or destruction of data. (see Section 9 on Security of Data)

8. Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Data must not be transferred outside of the European Economic Area (EEA) - the fifteen EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual. Members of the company should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

### Section 7: Data Subject Rights

Data Subjects have the following rights regarding data processing, and the data that are recorded about them:

To make subject access requests regarding the nature of information held and to whom it has been disclosed.

To prevent processing likely to cause damage or distress.

To prevent processing for purposes of direct marketing.

To be informed about mechanics of automated decision taking process that will significantly affect them.

Not to have significant decisions that will affect them taken solely by automated process.

To sue for compensation if they suffer damage by any contravention of the Act.

To take action to rectify, block, erase or destroy inaccurate data.  
To request the Commissioner to assess whether any provision of the Act has been contravened.

## Section 8: Consent

Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. The company understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists. In most instances consent to process personal and sensitive data is obtained routinely by the company (eg when a company member signs a registration form or when a new member of staff signs a contract of employment). Any company forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data are to be published on the Internet as such data can be accessed from all over the globe. Therefore, not gaining consent could contravene the eighth data protection principle.

If an individual does not consent to certain types of processing (eg direct marketing), appropriate action must be taken to ensure that the processing does not take place.

If any member of the company is in any doubt about these matters, they should consult the Company Data Protection Officer.

## Section 9: Security of Data

All staff are responsible for ensuring that any personal data (on others) which they hold are kept securely and that they are not disclosed to any unauthorised third party (see Section 11 on Disclosure of Data for more detail).

All personal data should be accessible only to those who need to use it. You should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:

in a lockable room with controlled access, or  
in a locked drawer or filing cabinet, or  
if computerised, password protected, or  
kept on disks which are themselves kept securely.

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.

This policy also applies to staff and company members who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and company members should take particular care when processing personal data at home or in other locations outside the

company offices.

## Section 10: Rights of Access to Data

Members of the company have the right to access any personal data which is held by the company in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the company about that person.

## Section 11: Disclosure of Data

The company must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff and company members should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of YMT business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of the company concerned.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

1. the individual has given their consent (eg a company/staff member has consented to the company corresponding with a named third party);
2. where the disclosure is in the legitimate interests of the institution (eg disclosure to staff - personal information can be disclosed to other company employees if it is clear that those members of staff require the information to enable them to perform their jobs);
3. where the institution is legally obliged to disclose the data (eg ethnic minority and disability monitoring);
4. where disclosure of data is required for the performance of a contract (eg informing a company members LEA or sponsor of course changes/withdrawal etc).

The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

to safeguard national security\*;  
prevention or detection of crime including the apprehension or prosecution of offenders\*;  
assessment or collection of tax duty\*;  
discharge of regulatory functions (includes health, safety and welfare of persons at work)\*;  
to prevent serious harm to a third party;  
to protect the vital interests of the individual, this refers to life and death situations.

\* Requests must be supported by appropriate paperwork.

When members of staff receive enquiries as to whether a named individual is a member of the company, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (ie consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of the company may constitute an unauthorised disclosure.

Unless consent has been obtained from the data subject, information should not

be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.

As an alternative to disclosing personal data, the company may offer to do one of the following:

pass a message to the data subject asking them to contact the enquirer;  
accept a sealed envelope/incoming email message and attempt to forward it to the data subject.

Please remember to inform the enquirer that such action will be taken conditionally: ie "if the person is a member of the company" to avoid confirming their membership of, their presence in or their absence from the institution.

Further information regarding the disclosure of personal information can be found in Appendices II (company member information) and III (telephone protocol). If in doubt, staff should seek advice from their Head of Department/Section or the General Manager.

## Section 12: Retention and Disposal of Data

The company discourages the retention of personal data for longer than they are required. Considerable amounts of data are collected on current staff and company members. However, once a member of staff or company member has left the company, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

### Company Members

In general, electronic company member records containing information about individual members are kept indefinitely and information would typically include name and address on entry and completion, projects participated in.

Departments should regularly review the personal files of individual members in accordance with the company's Records Retention Schedule (Appendix IV).

### Staff

In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held, leaving salary. Other information relating to individual members of staff will be kept by the Personnel Department for 6 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay etc will be retained for the statutory time period (between 3 and 6 years).

Departments should regularly review the personal files of individual staff members in accordance with the Company's Records Retention Schedule (Appendix IV).

Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for 12 months from the interview date. Personnel may keep a record of names of individuals that have applied for, be short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

### Disposal of Records

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (eg, shredding, disposal as confidential waste, secure electronic deletion).

### Section 13: Publication of Company Information

All members of the company should note that the company publishes a number of items that include personal data, and will continue to do so. These personal data are:

Names, job titles of members of staff.  
Internal Telephone Directory.  
Printed programmes and videos or other multimedia versions of projects.  
Information in programmes, annual reports, staff newsletters, etc.  
Staff information on the YMT website (including photographs).

It is recognised that there might be occasions when a member of staff, a company member, or a lay member of the company, requests that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, the company should comply with the request and ensure that appropriate action is taken.

### Section 14: Direct Marketing

Any department or section that uses personal data for direct marketing purposes must inform data subjects of this at the time of collection of the data. Individuals must be provided with the opportunity to object to the use of their data for direct marketing purposes (eg an opt-out box on a form).

### Section 15: Use of CCTV

The company's use of CCTV is regulated by a separate Code of Practice. For reasons of personal security and to protect company premises and the property of staff and company members, close circuit television cameras may be in operation in certain locations. The presence of these cameras may not be obvious. This policy determines that personal data obtained during monitoring will be processed as follows:  
any monitoring will be carried out only by a limited number of specified staff;  
the recordings will be accessed only by the General Manager and the Board of trustees;  
personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete;  
staff involved in monitoring will maintain confidentiality in respect of personal data.

### Section 16: Appendices

More detailed guidance on the following issues has been published by the company:

Appendices  
I: Staff Records Management  
II: Disclosure of Company Member Information  
III: Telephone Protocol for the Disclosure of Personal Information  
IV: Records Retention Schedule  
V: Photographs to be used in Publicity/Promotional Material

For further guidance or advice on the Data Protection Act, please contact the

General Manager: 08702405057

## Youth Music Theatre UK Data Protection Policy

### Appendices

Appendix I - Data Protection - Staff Records Management

Appendix II - Data Protection - Disclosure of Company Members Information

Appendix III - Data Protection - Telephone Protocol for the Disclosure of Personal Data

Appendix IV - Records Retention Schedule (records containing personal information) Data Protection

Appendix V - Guidance for Photographs to be used in Publicity/Promotional Material

### Staff Records Management Appendix I

The Data Protection Act 1998 gives individuals the right to access the information that an organisation holds on them. In order to comply with this part of the Act, organisations need to have in place effective means of extracting and retrieving information from a variety of sources.

In order to comply with a subject access request, departments/sections will need to be able to locate and collate the information quickly. It is therefore vital that key personnel (typically Head of Department, Line Manager and/or administrator) know what information is held and by whom.

Ideally, all information relating to individual staff should be kept in departmental staff record files (paper or electronic) so that, in the event of a subject access request, the department can be confident that all the information is easily accessible from a limited number of central sources.

However, YMT recognises that this may not always be the case in practice. Departments should ensure that staff record files are as complete as possible but it is acknowledged that there may be some instances where designated individuals need to retain information on staff which would not be appropriate for more general access.

The YMT has devised the following guidelines

1. Wherever possible, copies of documentation relating to an individual member of staff should be lodged in a departmental staff record file(s) (paper or electronic).
2. Designated individuals are permitted to retain duplicate copies of any documentation (electronic or paper), particularly if the information is consulted on a regular basis.
3. Exceptionally, designated individuals may also keep documentation relating to sensitive information (e.g. relating to health or other problems) without copying the information to the departmental staff record file. Designated individuals should only follow this practice when unauthorised access/disclosure of the information concerned to other staff in the department/section poses a risk of damage/distress to the member of staff.
4. Members of staff, other than those responsible for the staff record files and designated personnel, should **not** retain information (electronic or paper) about individual members of staff. Documentation should be filed either in the departmental staff record file or with a relevant designated individual.
5. The exception to this is email as it would be impractical for staff to pass all emails to a central source. However, all staff must be aware that in the event of a subject access request, they may be asked to search their email archives for all emails referring to the member of staff that has made the request. Therefore, staff are advised not to keep emails relating to other members of staff unless it is absolutely necessary. In writing emails referring to other members of staff, you are reminded that, in the event of a subject access request, that member of staff is entitled to receive copies of all emails which refer to them.
6. Information should only be retained in accordance with the suggested retention periods in the YMT's Records Retention Schedule.
7. When a designated individual leaves the YMT, they should pass all information to the member of staff responsible for staff files, to be either destroyed (in accordance with the YMT's records retention schedule), or filed on the departmental staff record file, or passed to a replacement designated individual.
8. Staff should be informed of what information is being held about them, what it will be used for, to whom it might be disclosed and whether or not it will be stored in the departmental staff record file.

If these guidelines are followed, personal information held on staff can be easily located from a limited number of sources and departments will be much better prepared to respond to subject access requests efficiently.

## Data Protection - Disclosure of Company Members Information Appendix II

The YMT must ensure that personal data held on company members are not disclosed to unauthorised third parties including family members, friends, government bodies and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on company members to third parties.

These guidance notes should be read in conjunction with the University's [Data Protection Policy](#), which includes a section on [Disclosure of Data](#).

This document is Appendix II to the Data Protection Policy.

---

### Section

1. [General Information](#).  
[Disclosing Personal Data](#) / [Disclosing Sensitive Personal Data](#) / [Disclosing Personal Data Overseas](#) / [Informing Company Members of Disclosures and Obtaining Consent / Requirement to Disclose?](#) / [Method of Disclosure](#).
  2. [Disclosure to Work Colleagues](#).
  3. [Disclosure to Relatives/Guardians and Friends](#).
  4. [Disclosure to current and prospective Employer and Educational Institutions](#).
  5. [Requests for Personal References](#).
  6. [Disclosures to the Police and Legal Proceedings](#).  
[Disclosures to the Police](#) / [Legal Proceedings](#).
  7. [Forwarding Company Member Correspondence on behalf of a Third Party](#).
- 

## Section 1: General Information

### Disclosing Personal Data

In accordance with Principle 1 of the Data Protection Act, personal data should only be disclosed if one of the conditions set out in Schedule 2 are met. The most likely conditions applicable to the disclosure of company member data to third parties are:

- i. the company member has given their consent
- ii. the disclosure is in the legitimate interests of the company or the third party to whom the information is being disclosed (except where this would prejudice the rights, freedoms or legitimate rights of the company member)
- iii. statutory obligation of the Company
- iv. disclosure is required for performance of a contract (eg contract between company member and sponsor)

### Disclosing Sensitive Personal Data

In accordance with Principle 1 of the Data Protection Act, sensitive personal data (racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions) should only be disclosed if one of the conditions set out in Schedule 2 (see above) AND one of the conditions set out in Schedule 3 are met. The most likely conditions (of Schedule 3) applicable to the disclosure of sensitive company member data to third parties are:

- i. the company member has given their explicit (ideally written) consent
- ii. statutory obligation of the Company (eg equal opportunities monitoring)
- iii. disclosure is in the vital interests of the company member (eg information relating to a medical condition may be disclosed in a life or death situation)

### Disclosing Personal Data Overseas

In accordance with Principle 8 of the Data Protection Act, personal data should only be disclosed outside of the EEA (the fifteen EU Member States together with Iceland, Liechtenstein and Norway) if one of the conditions set out in Schedule 4 are met. The most likely conditions applicable to the disclosure of company member data to third parties overseas are:

- i. the company member has given their explicit (ideally written) consent
- ii. disclosure is required for performance of a contract
- iii. disclosure is necessary for the purpose of any legal proceedings

## **Informing company members of Disclosures and Obtaining Consent**

Company members should be informed of predictable disclosures when they register with the Company. Some company members will choose to opt out of certain processing (including disclosures) on their registration form. This information is recorded on the Company database and all company member should check a company member 's record before releasing any information. In less predictable situations (eg parent phoning for financial details, taxi firm who has found wallet and wants to contact company member) where the company member has not been previously informed of a possible disclosure, the company member should give their consent before any information is released.

The Company understands "consent" to mean that the company member has signified their agreement whilst being in a fit state of mind to do so and without pressure being exerted upon them. There must be some active communication between the parties, consent cannot be inferred from non-response to a communication. In most cases, verbal consent should be acceptable so long as proper security checks are made to ensure that the person giving the consent is the company member. For telephone consent, this will mean asking the subject to confirm several separate facts that should be privy only to them (date of birth etc). For sensitive data, explicit written consent of company members should be obtained unless an alternative legitimate basis for processing exists (see above).

There are certain exemptions (Section 29) from the requirement to inform company members of disclosures if the information is being released for the prevention or detection of crime AND if informing the company member of the disclosure would prejudice the enquiries. See Section 2 for further detail.

### **Requirement to Disclose?**

Unless there is a legal or statutory obligation, you are advised not to disclose any personal information about company members without their consent. **Please note that disclosure includes confirmation of a company member's presence at the Company.** If you are in any doubt as to the legitimacy of a disclosure, then no disclosure should be made.

### **Method of Disclosure**

Disclosures should not be made over the telephone. The minimum security option is to take a number and ring the enquirer back. However, it is strongly advised that all enquirers should be asked to submit their requests in writing (where appropriate on headed paper). Once you have checked whether or not the request is legitimate, you should, wherever possible, reply in writing.

## **Section 2: Disclosure to Work Colleagues**

You should always think carefully before disclosing company members' personal information to work colleagues whether they be from within, or external to, your own department. Under the Data Protection Act, you should not disclose personal data to colleagues unless they have a legitimate interest in the data concerned. As there is no definition as to what a "legitimate interest" is, it will have to be a matter of judgement in each case. As a rule you should consider whether or not the information is necessary to allow your colleague to perform their job. So for instance, it would be legitimate to pass information to the Graduation Office regarding company member addresses and any disabilities if special arrangements were needed to enable the student to attend the project. When sharing information with colleagues, you should consider the level of detail necessary to enable them to perform their job. So for instance, if you knew that a company member was going to be absent for a significant period of time, you may wish to notify colleagues in the department of this fact. However, it might not be appropriate for all colleagues to be made aware of the specific reasons (health or otherwise) resulting in the absence.

## **Section 3: Disclosure to Relatives/Guardians and Friends**

The Company has no responsibility or obligation to disclose any personal information relating to company members to relatives, even if they are contributing to course fees.

All company members are given the opportunity, both on their registration form and by email later in the year, to provide the name of a nominated individual to whom the Company may disclose personal information. You should always check a company member's record to see whether or not they have identified a nominated individual. You may come under pressure to discuss individual students with parents/guardians or even friends. However, in these situations it is essential that you do not disclose personal data without the prior consent of the company member - it would be a

breach of the Data Protection Act to do so. If the company member has identified a nominated individual (see above) they are understood to have given prior consent.

You are, of course, free to discuss institutional procedures with parents (eg advising on when invoices should be paid by) but the specific circumstances of an individual company member cannot be discussed without the consent of that company member.

There may be occasional, exceptional circumstances (in which a company member's life or health is threatened) in which the usual need to get consent before disclosing to parents/guardians may be waived. The Company holds details of company members' "next of kin" for such purposes.

#### **Section 4: Disclosure to current and prospective Employers and Educational Institutions**

You may receive requests for information regarding individual company members (current or former) from current/prospective employers/educational institutions. Typically this occurs when the company member has applied for a job or a place on a programme of study. The disclosure will usually be in the best interests of the company member and more often than not, the company member will be aware that such a request would be made. The information released should be kept to a minimum. As always, care must be exercised in the method of disclosure (see Section 1). See Section 5 for more detail on Personal References.

#### **Section 5: Requests for Personal References**

If you receive a request for a personal reference relating to a company member, you should ensure that

- the information contained in the reference is **FACTUALLY** correct
- where possible, keep the disclosure to a minimum
- sensitive data (e.g. details of health to explain absences from the Company) must **not** be disclosed without the explicit consent of the company member
- where opinions about a person's suitability are disclosed, your comments are defensible and justifiable on reasonable grounds
- if you are unable or unwilling to give a reference, such a refusal is communicated carefully, without, in effect, implying a negative reference and thus disclosing personal data
- you do **not** disclose any information if asked to give an unsolicited reference (for a company member who has not, to your knowledge, cited your name as a referee)

The identity of the person requesting the reference should always be confirmed prior to disclosure. Requests for references should usually be made in writing on headed paper. If you receive an email request for a reference, you should be assured that it is a valid request. If it is from a known source or company domain, you should process the request but you may wish to reply in written format to a known postal address for the company/organisation. If the email domain is not familiar, you are advised to investigate further.

Telephone references are not usually recommended. However, they are acceptable if the company member has specifically asked you to provide a reference at short notice. As a minimum security measure it is recommended to ring the enquirer back to check that they are who they claim to be. If a company member cites your name as a referee, it is understood that they are giving consent for you to disclose information. **If you are not aware that a company member has cited you as a referee, you should check the validity of the request.**

#### **Section 6: Disclosure to the Police and Legal Proceedings**

##### **Disclosures to the Police**

Disclosures to the Police are **NOT** compulsory except in cases where the Company is served with a Court Order requiring information. However, Section 29 of the Data Protection Act 1998 does allow limited exemptions from the first Principle meaning that the Company may release information to the Police without the consent of company members in limited circumstances. Such disclosures should only be made if the Police confirm that they wish to contact a named individual about a specific criminal investigation and where the Company believes that failure to release the information would prejudice the investigation. Staff must not release information to the Police over the telephone. The Police must inform the Company in writing. Most Police Forces will have their own request form which should always include a statement confirming that the information requested is required for the purposes covered in Section 29, a brief outline of the nature of the

investigation, the company member's role in that investigation, and the signature of the investigating officer.

### **Legal Proceedings**

Section 35(2) of the 1998 Act exempts data from the non-disclosure provisions (eg obtaining consent from company members) in cases where disclosure is necessary "for the purpose of, or in connection with, legal proceedings.....or for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights". In practice this means that the Company can disclose information regarding company members to its own solicitors when seeking proper legal advice about a case. However, for cases that do not directly involve the Company, information should only be disclosed if the relevant company member's permission can be obtained. If the information is vital to a case, a Court Order may be issued demanding the information. Section 35(1) specifically allows data controllers to disclose without consent from the data subject (student) when confronted with a Court Order.

### **Section 7: Forwarding Company Member Correspondence on behalf of a Third Party**

You should not release company member addresses or contact details to a third party without the consent of the company member. Instead you may offer to forward correspondence to a company member on behalf of a third party. Sometimes you may even receive unsolicited correspondence with a request to forward it to a company member. You must take care when handling such requests. Remember that an individual's company member status is personal data. Therefore if you receive such a request it is important to neither confirm nor deny that that person is a company member of the YMT.

## **Data Protection - Telephone Protocol for the Disclosure of Personal Data Appendix III**

The Company must ensure that personal data held on individuals are not disclosed to unauthorised third parties including family members, friends, government bodies and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data to third parties. These guidance notes are intended to provide guidance for staff who deal regularly with telephone calls from third parties requesting personal data on company members and staff and should be read in conjunction with the Company's [Data Protection Policy](#).

This document is Appendix III to the policy.

### Section

1. [General Information on Disclosure of Personal Data](#).  
[Disclosing Personal Data](#) / [Disclosing Sensitive Personal Data](#) / [Disclosing Personal Data Overseas](#) / [Consent](#).
2. [Internal \(within company\) Disclosures by Telephone](#).
3. [External \(outside company\) Disclosures by Telephone](#).  
[General](#) / [Disclosure to Parents \(Company Member Information\)](#) / [Home Addresses, Telephone Numbers](#) / [References](#) / [Disclosures to the Police](#)
4. [Conclusion](#)

### Section 1: General Information on Disclosure of Personal Data

#### **Disclosing Personal Data**

In accordance with Principle 1 of the Data Protection Act, personal data should only be disclosed if one of the conditions set out in Schedule 2 are met. The most likely conditions applicable to the disclosure (over the telephone) of company member or staff data to third parties are:

- i. the company member or member of staff has given their consent.
- ii. the disclosure is in the legitimate interests of the company or the third party to whom the information is being disclosed (except where this would prejudice the rights, freedoms or legitimate rights of the company member or member of staff).
- iii. disclosure is required for performance of a contract (eg contract between a company member and their sponsor).

#### **Disclosing Sensitive Personal Data**

In accordance with Principle 1 of the Data Protection Act, sensitive personal data (racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions) should only be disclosed if one of the conditions set out in Schedule 2 (see above) AND one of the conditions set out in Schedule 3 are met. The most likely conditions (of Schedule 3) applicable to the disclosure (over the telephone) of sensitive company member or staff data to third parties are:

- i. the company member or member of staff has given their explicit (ideally written) consent.
- ii. disclosure is in the vital interests of the company member or member of staff (eg information relating to a medical condition may be disclosed in a life or death situation).

#### **Disclosing Personal Data Overseas**

In accordance with Principle 8 of the Data Protection Act, personal data should only be disclosed outside of the EEA (the fifteen EU Member States together with Iceland, Liechtenstein and Norway) if one of the conditions set out in Schedule 4 are met. The most likely conditions applicable to the disclosure (over the telephone) of company member or staff data to third parties overseas are:

- i. the company member or member of staff has given their explicit (ideally written) consent.
- ii. disclosure is required for performance of a contract.
- iii. disclosure is necessary for the purpose of any legal proceedings.

#### **Consent**

The YMT understands "consent" to mean that the company member or member of staff has signified their agreement whilst being in a fit state of mind to do so and without pressure being

exerted upon them. There must be some active communication between the parties, consent cannot be inferred from non-response to a communication. In most cases, verbal consent should be acceptable so long as proper security checks are made to ensure that the person giving the consent *is* the company member or member of staff. For telephone consent, this will mean asking the subject to confirm several separate facts that should be privy only to them (date of birth etc). For sensitive data, consent should NOT be obtained over the telephone and explicit written consent of company members or staff should be obtained unless an alternative legitimate basis for processing exists (see above).

### *Section 2: Internal (within Company) Disclosures by Telephone*

You should always think carefully before disclosing company member or staff personal information to work colleagues whether they be from within, or external to, your own department. Under the Data Protection Act, you should not disclose personal data to colleagues unless they have a legitimate interest in the data concerned. As there is no definition as to what a "legitimate interest" is, it will have to be a matter of judgement in each case. As a rule you should consider whether or not the information is necessary to allow your colleague to perform their job. When sharing information with colleagues, you should consider the level of detail necessary to enable them to perform their job.

If you can identify the member of staff making the telephone enquiry (eg from their voice) and you are satisfied that they have a legitimate reason for requesting the personal information, you may disclose this over the telephone. Take care to ensure that in disclosing the information over the phone, you are not inadvertently disclosing the information to other members of staff. This is particularly important in the case of sensitive personal data and for staff working in an open plan office.

If you cannot be sure of the identify of the member of staff making the telephone enquiry, you should ask them to put the request in writing (email is preferable) so that you can deal with it at a later stage. Again, before releasing the information, you need to be satisfied that the member of staff is requesting the data for a legitimate purpose. Ask the enquirer to indicate what they will be using the information for and keep the written communication as background evidence should the disclosure be questioned at a later date. To avoid embarrassment you could say that you do not have the information to hand and that you need time to find it and get back to them. Alternatively you could offer to take a contact telephone number and call them back later once you have gathered the information.

### *Section 3: External (outside Company) Disclosures by Telephone*

#### **General**

In general, disclosures to external bodies/companies/agencies/individuals should not be made over the telephone. It is strongly advised that you ask enquirers to submit their requests in writing (where appropriate on headed paper). This will give you time to check whether or not the request is legitimate and where possible obtain consent for the disclosure from the member of staff or company member about whom information is requested. You should, wherever possible, reply to the request in writing.

The company recognises that in some, exceptional situations, time constraints and other factors make it a necessity to disclose information over the telephone. Good practice is considered to be only releasing information to those individuals who know at least 3 identifying data (e.g. name, address and date of birth) about the data subject. This should minimise the potential for damages because a relationship between the data subject and the caller has been established. If you find yourself in a position where it is necessary to disclose information over the telephone, you should take a contact number and ring the enquirer back. This will go some way to ensuring that the caller is who they say they are. Even the above procedures could be subject to fraud and should only be used when no other alternative exists. In such cases, YMT should at least be regarded as having taken reasonable precaution given the circumstances - i.e. that the security in place was appropriate to the risk involved in unlawful processing of data. As always, particular care should be taken when disclosing sensitive personal data or information that could potentially cause the company member or member of staff to suffer subsequent damage and/or distress.

Please note that even confirming whether or not a company member or member of staff is part of or works for YMT could be a potential breach of the Act.

### **Disclosure to Parents (company member Information)**

YMT has no responsibility or obligation to disclose any personal information relating to company members to parents or other relatives, even if they are contributing to tuition fees.

You may come under pressure to discuss individual company members with parents/guardians or even friends over the telephone. However, in these situations it is essential that you do not disclose personal data without the prior consent of the company member - it would be a breach of the Data Protection Act to do so. If the company member has identified a nominated individual they are understood to have given prior consent.

You are, of course, free to discuss administration procedures with parents (eg releasing dates of performances, advising on when invoices should be paid by) but the specific circumstances of an individual company member cannot be discussed without the consent of that company member.

There may be occasional, exceptional circumstances (in which a company member's life or health is threatened) in which the usual need to get consent before disclosing to parents/guardians may be waived. The company holds details of company members' "next of kin" for such purposes.

### **Home Addresses, Telephone Numbers and E-mail addresses**

You should never give out **personal/home** addresses or telephone numbers of staff or company members to third parties over the telephone unless you have been given explicit (in writing) permission by the individual. Instead you could a) take the caller's contact details and say you will pass a message asking the company member or member of staff to contact them if they are in the Company or b) offer to forward correspondence to a company member or a member of staff on behalf of the caller. You must take care when handling such requests. Remember that an individual's company member/staff status is personal data. Therefore if you receive such a request it is important to neither confirm nor deny that that person is a company member or member of staff at YMT.

However, it would usually be deemed appropriate to disclose a colleague's **work** contact (telephone and departmental address) details in response to an enquiry regarding a particular function for which they are responsible. If you are asked to disclose another member of staff's email address, you should ask the caller to send the email to you and inform them that you will forward the message on to the individual they are trying to contact if they are a member of the Company. It would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter.

### **References**

Telephone references are not usually recommended. However, they are acceptable if you have been specifically asked by a company member or a member of staff to provide a reference at short notice. The identity of the person requesting the reference should always be confirmed prior to disclosure. As a minimum security measure it is recommended that you ring the enquirer back to check that they are who they claim to be.

When disclosing information in the form of a personal reference please ensure that:

- i. the information you disclose is **FACTUALLY** correct;
- ii. the disclosure is kept to a minimum (dates of participation/employment, positions held);
- iii. sensitive data (e.g. details of health to explain absences from the Company) are **not** disclosed without the explicit consent of the company member or member of staff;
- iv. where opinions about a person's suitability are disclosed, your comments are defensible and justifiable on reasonable grounds;
- v. if you are unable or unwilling to give a reference, such a refusal is communicated carefully, without, in effect, implying a negative reference.

### **Disclosures to the Police**

Disclosures to the Police are **NOT** compulsory except in cases where the Company is served with a Court Order requiring information. However, Section 29 of the Data Protection Act 1998 does allow the Company to release information to the Police **WITHOUT** the consent of company members or members of staff in **LIMITED** circumstances. Such disclosures should only be made if the Police confirm that they wish to contact a named individual about a specific criminal investigation and where the Company believes that failure to release the information would prejudice the investigation. If you are contacted by the Police and are not sure how to deal with

their request you can get in touch with the General Manager for advice on how to deal with the enquiry.

The Police MUST request the information from YMT in writing. You are NOT obliged to release information to the Police over the telephone. Most Police Forces will have their own request form, which should always include:

- i. a statement confirming that the information requested is required for the purposes covered in Section 29;
- ii. a brief outline of the nature of the investigation;
- iii. the data subject's role in that investigation;
- iv. the signature of the investigating officer.

#### Section 4: Conclusion

The purpose of the Data Protection Act 1998 is to protect the rights and privacy of individuals with regard to their personal information. At times you may feel like you are being obstructive to callers asking for information about company members or members of staff. In these cases, explain that the information falls under the Data Protection Act. Follow the above guidelines in a courteous and professional manner and in most circumstances you should not experience too many problems. However, if you are faced with a particularly difficult caller, do your best to diffuse the situation without losing your temper. Explain that you are following guidelines approved by the Copmany and that by providing the information over the telephone, you could be breaking the law. The Company has adopted some standard phrases to help you.

Remember:

- There is no such thing as a Data Protection emergency (except where someone's life or health may be at risk). You are well within your rights to stall a caller whilst you seek further information and advice.
- If in doubt ASK the General Manager.

Records Retention Schedule (records containing personal information) Appendix IV

The following minimum retention periods relate to all personal information, regardless of the format in which it is stored. The list is not exhaustive, but provides guidance as to best practice.

[Health and Safety Records](#)  
[Employee Records](#)  
[Company Member Records](#)

Applications

[General](#) company member files collated during project

Discipline, appeals and complaints

**Health and Safety Records**

Type of Record	Minimum Retention Period	Location	Reason for Length of Period
Pre-employment health screening questionnaire	During employment plus 3 years	Occupational Health	Management of Health and Safety at Work Regulations 1999
Occupational Health Records - health surveillance and medical records relating to risk assessments or incidents occurring at work	40 years	Occupational Health/Health, Safety and Environment Office	Management of Health and Safety at Work Regulations 1999 Noise at Work Regulations 1989
Occupational Health Records where reason for termination of employment is connected with health, including stress related illness	During employment plus 3 years	Personnel, Occupational Health	Limitation period for personal injury claims (there may be circumstances where it is not practical to separate these from other Occupational Health Records)
Health surveillance and medical records plus air monitoring and/or biological monitoring etc. kept by reason of the Control of Substances Hazardous to Health Regulations 2002	5 years or 40 years in respect of specific individuals	Health, Safety and Environmental Office	Control of Substances Hazardous to Health Regulations 2002
Records relating to asbestos, medical records, training records, suspect incidents of potential exposure	40 years	Estates, Health, Safety and Environmental Office	Control of Asbestos at Work Regulations 2002
Ionizing Radiation Records	50 years after last entry	Radiation Protection Officer	Ionizing Radiations Regulations 1999

**Employee Records**

Type of Record	Minimum Retention	Location	Reason for Length of Period
----------------	-------------------	----------	-----------------------------

	Period		
Facts of employment (dates of appointments, positions held etc)	Perpetuity	Personnel Services, HoD	Provision of references and requests for confirmation of employment.
All personnel files EXCLUDING information on disciplinary and/or grievance proceedings (but including health information, application forms and references)	6 years from the end of employment	Personnel, Staff Development, HoD	Provision of references and potential litigation.
Staff Discipline		HoD copied to Personnel if appropriate	
Oral/verbal warning - brief note on file (subject to satisfactory conduct and performance)	6 months		In accordance with Conditions of Service
Written warning - including notes of disciplinary hearings kept on file (subject to satisfactory conduct and performance)	First Warning 12 months Final Warning 2 years		In accordance with Conditions of Service
Documentation relating to grievance hearings (notes, reports etc) NOTE: Grievance Committee members must hand in all paperwork at the end of a meeting/hearing to avoid retention of duplicate documents	2 years	HoD copied to Personnel if appropriate	Allows for appropriate appeal mechanism and monitoring future grievances
Application forms and references for unsuccessful candidates	12 months	HoD	Feedback to applicants Time limits on litigation
Interview Notes (all Appointment Committees' members' notes to be handed to single person at end of interview)	12 months	HoD	Feedback to applicants and time limits on litigation
Facts relating to redundancies:			
Where less than 20 redundancies	6 years from the date of redundancy	Personnel	Time limits on litigation
Where 20 or more redundancies	12 years from the date of the redundancies	Personnel	Limitation Act 1980
Income Tax and NI Returns, including correspondence with tax office	6 years after end of the financial year to which the	Payroll, Finance	Income Tax (Employment) Regulations 1993

	records relate		
Statutory Maternity Pay records and calculations	6 years after end of the financial year to which the records relate	Payroll, Personnel	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	6 years after end of the financial year to which the records relate	Payroll, Personnel	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	6 years	Payroll, Finance	Taxes Management Act 1970
Accident books, and records and reports of accidents	3 years after the date of the last entry	HoD, Health & Safety Officer	Social Security (Claims and Payments) Regulations 1979; RIDDOR 1985

### Company Member Records

Type of Record	Minimum Retention Period	Location	Reason for Length of Period
<b>APPLICATIONS</b>			
Records documenting the handling of enquiries from prospective company members	Current Year + 1 year	Pastoral	Good practice
Records documenting the handling of applications for admission: unsuccessful applications	Current Year + 1 year	Pastoral	Good practice
Records documenting the handling of applications for admission: successful applications	Current Year + 1 year	Pastoral	Good practice
<b>GENERAL COMPANY MEMBER FILES COLLATED DURING PROJECT</b>			
All personnel files EXCLUDING information on disciplinary and/or grievance proceedings (but including health information, application forms and references)	6 years from the end of project	Pastoral	Good Practice
<b>DISCIPLINE, APPEALS AND COMPLAINTS (held separately from main student file)</b>			
Records documenting the conduct and results of disciplinary proceedings against individual company	Last action on case + 6 years.	Pastoral	Limitation period for negligence.

members.			
Records documenting the handling of formal complaints made by individual company members.	Last action on case + 6 years.	Pastoral	Limitation period for negligence.
Records documenting the handling of complaints made by individual company members where formal complaints procedure is not initiated.	Last action on case + 3 years.	Pastoral	Good practice.

For further guidance, please contact the General Manager

## Data Protection - Guidance for Photographs to be used in Publicity/Promotional Material Appendix V

These guidance notes cover the provision and receipt of references for both staff and company members and should be read in conjunction with the company's Data Protection Policy. This document is Appendix V to the policy.

### **General Photographs**

If individuals are not readily identifiable from the photograph and it seems unlikely that any damage or distress will result from such processing then it will not be necessary to obtain consent. Therefore, company members and staff whose images appear as incidental detail in publicity photographs will not need to give consent for the use of their image.

### **Photographs of Group Activities**

Where photographs are to be taken of a group activity (e.g. a workshop) then this should be announced in advance so that individuals may leave the room briefly if they do not wish to appear in the photographs.

### **Photographs of Small Groups/Individuals**

Where photographs are to be taken of a single individual, or a small group of individuals, where individuals are the main subject of the photograph (even if they are not identified by name), consent should be sought before any photographs are taken. When gaining consent, it is important to ensure that individuals are informed of what the images will be used for (e.g. where they will be printed and who will have access to them). In most cases, verbal consent is all that will be required although photographers may wish to use a standard release form, to be signed by the subject(s), to ensure that they have appropriate consent.

### **Publishing Photographs on the Web**

If it is intended to make photographs available on the web. Publishing on the Internet potentially transfers personal data outside of the EEA (the fifteen EU Member States together with Iceland, Liechtenstein and Norway) for which rules on gaining consent from individuals are much stricter. If photographs (except where company member/staff images appear as incidental detail) are to be published on the Internet, written consent should be obtained from the subject(s) on a standard release form.

For further guidance, please contact the General Manager.

---