ROYAL CENTRAL
SCHOOL OF SPEECH & DRAMA

UNIVERSITY OF LONDON

DATA PROTECTION AND RECORDS RETENTION HANDBOOK

Contents

SECTION 1: INTRODUCTION 4
KEY RESPONSIBILITIES AND CONTACTS 4
HANDBOOK REVIEW 4
SECTION 2: OVERVIEW 5
LEGISLATIVE FRAMEWORK 5
DEFINITIONS 5
PRINCIPLES 6
SECTION 3: STAFF RESPONSIBILITIES 8
YOUR RESPONSIBILITIES TO CENTRAL AS AN EMPLOYEE 8
SECTION 4: INFORMATION FOR STUDENTS 10
WHAT DATA IS HELD? 10
WHAT IS IT USED FOR? 10
YOUR OBLIGATIONS 11
SECTION 5: SPECIFIC GUIDANCE FOR USERS 12
GENERAL PROTECTION OF DATA 12
THE USE OF PERSONAL MOBILE DEVICES 12
EMAIL SECURITY 13
VIRUSES AND SPYWARE 14
DISCLOSURE OF DATA TO THIRD PARTIES 14
PARENTS AND RELATIVES 14
IMMIGRATION OFFICIALS 15
THE POLICE AND OTHER OFFICIALS 15
QUALIFICATION CHECKS 15
SHARING INFORMATION WITH COLLEAGUES 15
TRANSFER OF DATA OUTSIDE OF THE EU 15
EXAMINATION MARKS 16
RELEASE OF EXAM MARKS TO DEBTORS 16
EXAMINATION PASS LISTS 16
EXAMINATIONS SCRIPTS 16
EXAMINERS' COMMENTS 16
PERSONAL DATA AND RESEARCH 17
DATA PROCESSING 17
EMPLOYING STUDENTS 17
KEEPING FILES ON INDIVIDUALS 18
COLLECTING INFORMATION FROM CHILDREN 18
PERSONAL INFORMATION ON THE SCHOOL WEBSITE 18
PHOTOGRAPHS 18
WORKING FROM HOME 19
PRIVACY NOTICES 19
SECTION 6: DATA SUBJECT RIGHTS 21

RIGHT TO BE INFORMED 21
RIGHTS OF ACCESS, DATA PORTABILITY AND ERASURE 21
WHAT DO I DO IF I RECEIVE A REQUEST? 22
RIGHT TO RECTIFICATION 22
RIGHTS TO RESTRICT PROCESSING AND TO OBJECT 22
RIGHTS RELATED TO AUTOMATED DECISION MAKING 22
COMPLAINTS 22

SECTION 7: DATA BREACH PROCEDURE 23

INTRODUCTION 23
PROCEDURE FOR REPORTING DATA BREACHES 23
REVIEW OF DATA BREACH PROCEDURES 23

SECTION 8: RECORDS RETENTION 24

RECORDS WHICH MAY BE ROUTINELY DESTROYED 25
ACADEMIC REGISTRY 26
STUDENT FILES 26
DEVELOPMENT AND EXTERNAL AFFAIRS 29
ESTATES / OPERATIONS 33
FINANCE 34
GOVERNING BODY 35
HUMAN RESOURCES 37
IT 39
LEARNING CENTRE 40
LIBRARY 42
RESEARCH OFFICE 43
TECHNICAL SUPPORT DEPARTMENT 45

APPENDICES 48

APPENDIX 1: SUBJECT ACCESS REQUEST FORM 48
APPENDIX 2: DATA BREACH REPORT FORM 51
APPENDIX 3: CONTENTS OF HUMAN RESOURCES FILES (STAFF) 54
APPENDIX 4: CONTENTS OF ACADEMIC REGISTRY FILES (STUDENTS) 55
APPENDIX 5: CONTENTS OF LEARNING CENTRE FILES 58
APPENDIX 6: WRITING REFERENCES FOR STUDENTS AND FORMER STUDENTS 59
APPENDIX 7: WRITING REFERENCES FOR STAFF MEMBERS 62

Authored/Modified by	**Data Protection Officer**
Date	**19 October 2018**
Date confirmed	**26 November 2018**
Version	**2.0**

Section 1: Introduction

The Royal Central School of Speech and Drama, University of London (Central), is committed to protecting the privacy of all those individuals – including, but not limited to, its students, staff, alumni, donors, and visitors – whose personal data it collects and processes.

The principles and procedures that are outlined in this document, and which apply throughout the institution, aim to ensure that the School treats all personal data safely and responsibly and that it complies fully with all legislation pertaining to data protection.

The Handbook should be read in conjunction with Central's Data Governance Policy, which describes the arrangements for the governance and assurance of the management and quality of data across the School.

Key Responsibilities and Contacts

Everyone who handles personal data in any capacity – whether they are a member of staff, a visitor, or a student – has a basic responsibility for ensuring that that data is treated sensitively and with due regard to the rights of the individuals concerned. Specific obligations and responsibilities are described in greater detail later in this document.

Data protection-related issues and procedures at Central are overseen and managed by a **Data Protection Officer**. General queries about data protection, or specific questions about the content of this Handbook, should be directed to them at dataprotection@cssd.ac.uk, or in writing to The Royal Central School of Speech and Drama, 62-64 Eton Avenue, London NW3 3HY.

Handbook Review

This Handbook is reviewed and updated annually.

The most recent review took place in June 2018.

Section 2: Overview

Legislative Framework

The Data Protection Act 1998 (DP Act 1998) established a framework of rights and duties which was designed to safeguard personal data. This framework sought to balance the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect the privacy of their personal details.

In May 2018, the DP Act 1998 was superseded by the General Data Protection Regulation (GDPR) and by a new UK Data Protection Act (DP Act 2018). Although the new legislation shares many of the DP Act 1998's main principles, it also introduces new elements and amplifies some existing concepts. In particular, GDPR makes more explicit the principles of accountability and transparency in relation to the processing of data and compliance with the legislation, and provides a more detailed definition of 'personal data', with a wider range of personal identifiers (including IP addresses).

It is also worth noting that the fines that can be imposed on organisations that are found to be non-compliant or in breach of their responsibilities under GDPR are significantly greater (up to 4% of annual global turnover or €20 million).

Definitions

The following terms and definitions are taken directly from the GDPR (Chapter 1, Article 4).

Personal data means any information relating to an identified or identifiable natural, living person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[Note that the GDPR refers also to ***special categories*** of personal data (or sensitive data) that include a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data and biometric data, and data concerning health, sex life or sexual orientation.]

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis. [Note that this encompasses both automated and manual filing systems.]

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controller *(or* ***data controller****)* means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processor (or **data processor**) means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Principles

The following principles relating to the processing of personal data have been taken from the GDPR (Chapter 2, Article 5).

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject.

In practice, this means that you must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified and adverse effects on the individuals concerned;
- be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle peoples' personal data only in ways they would reasonably expect; and
- make sure that you do not do anything unlawful with the data.

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

In practice, this means that you must:

- be clear from the outset about why you are collecting personal data and what you intend to do with it;
- comply with relevant fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;
- ensure that if you wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

In practice, this means that you should ensure that:

- you hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual;
- you do not hold more information than you need for that purpose;
- you identify the minimum amount of personal data you need to properly fulfill a purpose. You should hold that much information, but no more (this is part of the practice known as 'data minimisation').

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

To comply with this principle you should:

- take reasonable steps to ensure the accuracy of any personal data you obtain;
- ensure that the source of any personal data is clear;
- carefully consider any challenges to the accuracy of information.

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

In practice, it means that you will need to:

- review the length of time you keep personal data;
- consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes;
- update, archive or securely delete information if it goes out of date.

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In practice, this means that you must ensure appropriate security to prevent the personal data we hold from being accidentally or deliberately compromised. In particular, you will need to:

- design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach;
- be clear about who is responsible for ensuring information security;
- make sure the right physical and technical security is in place, backed up by robust policies and procedures and reliable, well-trained staff;
- be ready to respond to any breach of security swiftly and effectively.

It is a requirement that data controllers are both responsible for, and able to demonstrate compliance with, these principles.

Section 3: Staff Responsibilities

As noted in the Introduction, everyone who handles personal data has a responsibility to ensure that it is treated sensitively and with due regard to the rights of the individual.

It is the School's aim to ensure that all staff have at least a basic understanding of the impact of data protection requirements and legislation, and the potential consequences of non-compliance. In worst cases, the Information Commissioner can impose financial penalties and bring individual criminal charges. With such potential serious risk to the business and individuals, the School is committed to ensuring that its staff have an appropriate level of understanding of the legislation so as to ensure compliance with the law.

Central's Data Governance Policy provides further details of the specific duties of those with responsibility for the operational management and processing of data sets within the institution.

Your Responsibilities to Central as an Employee

What follows is a general account of the responsibilities of Central's staff in relation to their own and others' personal data. Data subject *rights* – including those of staff – are outlined in Section 6.

In relation to your own data:
You should ensure that you update your personal details on JANE (i.e. changes of address and emergency contact details) as the need arises. Human Resources (HR) cannot be held responsible for any errors or omissions. You must check that any information provided to you by HR in connection with your employment is accurate and up to date.

HR will advise you of the type of personal information held about you, as well as the reason for any processing of that information, including by the Higher Education Statistics Agency (HESA). Further information can be found on the Personal Details page on JANE and on the HESA website (the 'Staff collection notice').

In relation to the personal data of others:
You must supply, on request, to the Data Protection Officer information relating to all personal data held or used by you in electronic or manual format in connection with your employment by the School.

In general terms:
Staff members controlling personal data should ensure that the following requirements are complied with at ***all times****:*

- data that is processed by a third party will normally require a data protection agreement to be in place;
- staff working with the data are familiar with the relevant legislation and know what disclosures are permitted;

- the personal data is accurate and kept up to date for the purpose for which it is being used;
- when collecting personal data, the data subject should be made aware of the reason that the data is collected, its use, how long it will be retained and to whom it will be disclosed;
- data collected and held should be adequate, relevant and not excessive in relation to the purposes for which it has been collected. All data must be deleted or destroyed when no longer required, subject to the retention schedule (see Records Retention, below).
- data is collected fairly and used for the purpose for which it is collected. Additional data must not be collected "in case it might turn out to be useful later on";
- even if personal data is collected from publicly available sources (e.g. Electoral Roll, Telephone Directory, Who's Who) the use must be registered;
- in the absence for more than a short period of the person controlling the data, information on how to obtain data in response to data subject access enquiries is lodged with the Data Protection Officer or your Line Manager;
- data is kept securely and cannot be accessed by or disclosed to unauthorised persons. This includes any processing of Central data off campus;
- data breaches should be notified immediately to the Data Protection Officer (refer to Section 7, below, for more details about the procedure);
- precautions are taken to ensure that personal data is not accidentally lost or destroyed;
- use of personal data by students complies with the guidance set out below.

In relation to staff working with students:

- Advise the student about the requirements of the legislation.
- Ensure that students comply with the legislation by:
    a) implementing any instructions issued by you in relation to data;
    b) complying with the General Protection of Data (see Section 4);
    c) consulting with you in any case of doubt over interpretation of the legislation and the use of data;
    d) supplying to you the means by which data can be retrieved.
- Ensure that the use of personal data is registered – consult with the Data Protection Officer about this.
- Ensure that the data is deleted or destroyed when it is no longer required (see also Records Retention, below).

In relation to other personal data:

If you hold personal data on individuals other than Central staff or students, you must:

a) Advise the data subject of:

- what information you hold and what it will be used for;
- the responsibility of the data subject in supplying correct information and any amendments to such information;
- information on access.

b) Obtain the data subject's consent to process.

Section 4: Information for Students

What data is held?

Central holds and processes the following information in electronic and/or paper form:

- personal details
- academic record
- finance details
- disabilities
- eligibility for Disabled Student Allowance
- medical reports
- Students' Union membership
- information on criminal records
- disciplinary action
- details of appeals and complaints

Your student record is based on your application form (including, in the case of undergraduates, the UCAS application) and registration form. Further information is added to the record throughout your time at Central.

More details can be found in the School's Student Privacy Notice.

What is it used for?

The data is used for matters relating to your registration as a student of Central. Records will be retained when you leave Central and may be used for Alumni and reference purposes.

Central is required to provide information to external bodies such as the Higher Education Statistics Agency (HESA), grant awarding bodies, Student Loans Company, local authorities for Council Tax and Electoral Roll purposes, and, under the terms of the relevant legislation, to the Police or officers of the Courts if required to do so.

You can find details of how your information is used by HESA and for what purposes on the HESA website (the 'Student collection notice'); a link is also provided on MyCentral.

Basic details of your student record are deemed to be public information and will be used, for example, in publicity materials and in the graduation programme. Central will, with your consent, confirm award results to third parties (e.g. prospective employers) on request, and your progress to funding bodies (including overseas sponsors). You may, with good reason and under certain condition, request that certain details of your student record not be made public or that the information that Central holds about you is erased entirely. See Section 6 ('Your Rights') for more information.

Your record may also contain details of any warnings given or disciplinary action taken against you for breach of School regulations. The School may disclose this and any other related personal information, medical information and any data concerning your criminal record to members of School staff or to outside organisations or individuals with whom you

may have contact (such as those offering work placements) if the School deems it necessary and proportionate in order to safeguard you or others: for example, where a failure to do so would breach its stated responsibilities under its Safeguarding Children and Vulnerable Adults Policy.

Audio and video recording of classes may be permitted for disabled students as a reasonable adjustment. It is a requirement that the student notify the other attendees. This is to enable other attendees to express their wish not to be recorded and for the recording to be paused during their participation. Students who record classes are subject to the following conditions:

- you can only use recordings for your own study;
- you must not share these recordings with any third parties;
- you must not upload these recordings on to any public website.

Non-compliance with these conditions will be treated as a serious breach of conduct, resulting in action being taken under the Student Disciplinary Procedures.

Your obligations

The School is required to ensure that the information it holds is accurate and up-to-date. It must, however, rely on students to inform the appropriate office of any change in their personal data. In particular, any change of home or term-time address should be notified to the Student Advice Service.

As a user you are required to comply with Central's regulations for the use of computing facilities. It is also your responsibility, should you hold personal data on others, to ensure that you abide by the terms of the legislation and the principles of data collection, as outlined in this Handbook.

Section 5: Specific Guidance for Users

General protection of data

Users must take all reasonable steps to ensure the security of personal data, and in particular should ensure:

- computers which are used by staff to access personal data should not be placed in public areas where unauthorised persons can read the screens;
- personal files should be kept in locked filing cabinets. Never leave personal information lying on your desk. If possible clear all papers off your desk each evening and file them away or lock them in a desk drawer or cupboard for safekeeping overnight;
- when you leave your workstation it is good practice to 'lock' it (just hit CTRL-ALT-DEL and click on 'lock computer'). This ensures that no one can use your PC while you are away from your desk. It only takes a second or two and keeps information on your PC secure;
- USB sticks, other media and printed data should be locked away when not in use and not left in public areas;
- unwanted material should be shredded and placed in a secure waste bag. Arrangements for the collection and shredding of secure material should be made with the Estates team;
- where practicable, and particularly with highly sensitive material, data should be de-personalised or encrypted;
- computer passwords should not be easily deduced and should be changed regularly;
- when data on CDs and removable hardware are no longer required, it should be completely overwritten or erased;
- where data is downloaded from the student records system to computers, it should not be copied and used elsewhere and must not be kept longer than necessary for the purpose for which it is being used. Data from this source must not be used to satisfy access requests since it is a copy and may be out of date;
- avoid taking personal information home with you. If you need to save personal data onto a laptop or removable storage (e.g. memory stick) then ensure it is encrypted.

The use of personal mobile devices

With developments in smart phone technology and mobile devices such as tablets, more Central employees are opting to access emails and connect to the School network remotely.

Working from a coffee shop may seem like a nice idea, but using its Wi-Fi hotspot or any other open public network may jeopardise sensitive data. You should therefore not use public Wi-Fi hotspots.

It is vital that you do not save any personal data onto your home computer and that you ensure that no-one else in your household is able to access any information. If you use a home computer for work purposes, you must have up-to-date anti-virus software installed and ensure you apply all security updates to your computer operating system.

If you choose to use your personal device for work then you must ensure that your device is password protected with a strong password including upper and lower case characters along with at least one number. Passwords should be reset at least every 60 days. Your phone should be set to 'time out' after a short period of inactivity, so it will be harder to access if it falls into the wrong hands. Consider encrypting the data on your mobile device through the built-in operating system or third-party software. Your service provider may also be able to lock a lost or stolen device remotely or wipe the data from it. In addition to this you should always remember to lock your device when it is not in use.

Like any other computing device, smartphones are susceptible to technical failure. Because of their smaller size, they are also more likely to be lost, stolen or broken. All staff should use One Drive for Business, as provided by the School, which ensure that all business-critical data is being saved in the Cloud.

Ensuring that all smartphone applications are up-to-date can also help protect your mobile devices from malware and viruses that target vulnerabilities in their operating systems or browsers. Many smartphones can be set so users are notified by email when new software is available.

Generally, the same rules that are applied to working at your PC should be applied to your mobile device, so avoid opening suspicious emails, attachments or applications, and do not open links on dubious web pages.

Please note that connecting your personal computer and/or mobile device to the Central network is entirely at your own risk. The School will not be liable for any loss, damage or inconvenience arising directly or indirectly to a personal computer and/or mobile device as a result of its connection to the network. Although the School takes reasonable care to prevent the corruption of information, it does not give any warranty or understanding to the user about the integrity of information.

The School accepts no responsibility for the malfunctioning of a personal computer and/or mobile device, its hardware or software as a result of its connection to the Central network.

The School accepts no responsibility for the loss of any data or the failure of any security or privacy mechanism on a personal computer and/or mobile device that has been connected or is connected to the Central network.

Email security

- Consider whether the content of an email should be placed in an encrypted or password protected attachment. ***Note:*** If you do encrypt any emails, you will need to be confident that you can access them if asked to produce them for a subject access request.
- It is also a good idea to turn off the 'suggest names' facility on Outlook. This means you have to type in the address in full or look it up in the address book. This small inconvenience mitigates the risk of sending information to the wrong person.

- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.
- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
- If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message.

Viruses and spyware

- Make sure that your operating system is set up to receive automatic updates.
- Protect your computer by downloading the latest patches or security updates, which should cover vulnerabilities.
- Take regular back-ups of the information on your computer system and keep them in a separate place so that if you lose your computers, you do not lose the information.
- Securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk).
- Consider installing an anti-spyware tool. Spyware is the generic name given to programs that are designed to secretly monitor your activities on your computer. Spyware can be unwittingly installed within other file and program downloads, and their use is often malicious. They can capture passwords, banking credentials and credit card details, and then relay them back to fraudsters. Anti-spyware helps to monitor and protect your computer from spyware threats, and it is often free to use and update.

Note: *staff managed desktops will take care of security issues automatically.*

Disclosure of data to third parties

Data protection legislation protects the data subject from their data being disclosed to or processed by unauthorised third parties. Unauthorised third parties include:

- a person or organisation to whom the data subject has not consented that the data be disclosed;
- a person or organisation to whom the data subject has consented that the data be disclosed, but where the request is for reasons other than that for which the data was collected, or for which the consent was given.

Unauthorised third parties will include family members, friends, local authorities, government bodies and the police, unless non-disclosure is exempted by the legislation.

Parents and relatives

The general rule is that students and staff are private individuals and the School has no responsibility or obligation to keep their relatives informed of any aspect of their studies,

professional activities, or private lives. Therefore when a parent insists that Central staff provide them with information relating to their son/daughter, staff must say that because of data protection legislation they are not allowed to give out any information about any of our students. If a student wishes us to share information with their parent(s), they will be required to sign a consent form.

Immigration Officials

The School sometimes receives requests from immigration officials about individuals either studying at or on their way to the Central. Please pass all these enquiries on to the Admissions and Student Recruitment Office.

The Police and other officials

Occasionally, the School receives requests from the police and officials for personal information. If you receive a request from the police, you should always refer this request to the Data Protection Officer.

'Other officials' includes benefit fraud agencies trying to confirm that claimants are students and entitled to make claims, or immigration officials checking that a person is a student sponsored by the School. In all these cases you should refer to the Data Protection Officer.

Qualification checks

Employers, recruitment agencies, other HE providers, and other similar bodies regularly ask for information about our students. Normally they are asking for us to confirm qualifications or provide references so that they can consider a student for a job or a place on a course.

All such requests should be referred to the Academic Records Office.

Sharing information with colleagues

The School is a single 'Data Controller', so passing information about staff or students between staff does not include a 'third party'. However, this does not mean that information can be shared freely. There should be a good reason for the information to be shared, and the minimum amount of information should be shared each time. It is particularly important to make sure that information about sensitive issues, including disability, sexuality or ethnicity is not shared unless it is absolutely necessary.

If you pass information through e-mail or internal post you need to make sure that it will safely reach the person you mean to send it to, and will not accidentally be seen by anyone else. This means checking the name in the e-mail 'to' box carefully before hitting 'send' or writing the name and department clearly on an envelope. Envelopes and e-mails should be marked 'confidential' where the content relates to personal data. You should avoid faxing personal information as this is not secure or confidential.

Transfer of data outside of the EU

Personal data shall not be transferred to a country or territory outside the EU or 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.

If the School enters into partnerships with overseas organisations it may have to provide details about staff, students or alumni to that organisation. This is permitted only if the country has its own protections which are of a similar standard to the European ones.

You must consult the School's Data Protection Officer in all such cases.

Examination marks

Students have the right to see preliminary marks and comments that contribute to final assessments, if they ask to see them. If a student submits a Subject Access Request (see section below), the School has to provide access to all examination marks either within five months of the request (if the results have not yet been published) or one month after the official release of results - whichever is sooner. The delay is to stop students trying to find out what their marks are before the results are made official.

Release of exam marks to debtors

If a student remains in tuition fee debt to the School at the time when his/her result would usually be available, the student will be excluded from any pass list, no transcript will be released, the degree will not be conferred and no personal reference is to be supplied.

Should a student make a Subject Access Request for information concerning results, the School will provide the information but will annotate the information to the effect that the degree has not been conferred; the information statement is not a formal transcript; that the student at the time of the access request was indebted to the School; and that the information has been supplied in response to an access request.

Examination Pass Lists

You should not post personal information on notice boards, including pass or results lists.

Examinations scripts

Higher Education Providers do not have to provide exam scripts or the information recorded in them. However, examiners' comments are not covered by this exemption.

Examiners' comments

Students have a right to see comments made by internal and external examiners. This means that comments must be intelligible and appropriate. It is helpful if examiners' comments are made on separate comment sheets, rather than directly on exam scripts. Examiners need to be made aware of this in advance. If comments are handwritten and potentially illegible, it may be necessary to supply a typed version. If the examiners' comments have been made directly onto the exam script itself, the student cannot see the script so the comments would have to be transferred to a separate sheet that the student is allowed to see. ***Note:*** be careful not to write anything inappropriate as this would have to be released to a student if requested by them, regardless of what is written.

Personal data and research

Central supports the principle of open research, and is committed to sharing research data where appropriate and possible.

Data protection legislation applies to people collecting or using personal information as part of research. It is important that if you collect personal information as part of your research you explain to people what you are collecting, why you are doing it, what you will do with the information. Remember to tell them about all the things you will do with their information. You may be collecting for a PhD thesis now, but if you are intending to publish that as a book later, then let people know.

Further information can be found in the School's Research Conduct and Ethics Handbook.

There are some parts of the legislation that do not apply in quite the usual way when information is being collected for research. In particular, organisations that process personal data for research purposes may avoid restrictions on secondary processing and on processing sensitive data. As long as they implement appropriate safeguards, such organisations may also override a data subject's right to object to processing and to seek the erasure of personal data.

Data processing

A 'Data Processor' is someone other than a Central staff member who processes data for and on behalf of the School. In such cases:

a) ensure that the processing is carried out under a contract:
    i. which is made or evidenced in writing; and
    ii. under which the data processor is to act only on instructions from the data controller; and
    iii. which requires the data processor to comply with obligations around the unauthorised or unlawful processing of data and its accidental loss or destruction;
b) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out; and
c) take responsible measures to ensure compliance with those measures.

You should consult with the Data Protection Officer for support in developing a contract with a third party data processor and related matters.

Employing students

The School sometimes employs registered students. If you employ a student, you need to make sure that as part of their induction they are told about the importance of data

protection and understand that the information about students or staff that they have access to has to be treated confidentially.

Keeping files on individuals

The School keeps files of relevant information on staff and students. Everyone has a right to ask to see the information we keep about them. This means that you need to think carefully about the information you keep about people. It does not mean you can only ever write positive things about people on their file. It does mean that you should always use balanced and measured language in what you write. You should stick to facts, not opinions. Where you do need opinions then you should clearly state that that is what they are. You should never make notes that are rude, offensive, derogatory or damaging.

Information about someone does not need to be in an actual physical file for them to ask to see it. It can be an e-mail or electronic document. This means that you should think carefully about what you put in e-mails. See the e-mail guidance earlier in this Handbook for more information.

Collecting information from children

If you need to collect personal data from children, you should ensure that any information you provide to them about their rights and the uses to which their data will be put is set out clearly and accessibly. For children under 13 years old, you will need to get the consent of whoever holds parental responsibility for them before collecting and processing their data.

You should inform the Data Protection Officer (dataprotection@cssd.ac.uk) if you intend to collect personal data from children.

Personal information on the School website

The website is a public space. We generally publish information about people's official roles and functions. This helps those who need to deal with the School to find the right person to contact. It can also promote the School by letting people see which high profile academic staff we employ.

It is important that anybody whose name and other information appears on the website knows that it is there and that there are ways for them to object and for the information to be removed if needs be.

Photographs

A photograph of a person is 'personal data'. People have the right to refuse to have their photograph or personal information published, even if it can only be seen by people on campus. It is best to ask people before you make their picture and details public. Even

though the information is likely to be work related and not to do with their private life it still counts as personal information.

Working from home

If you work from home you still have to abide by the data protection principles outlined in this Handbook. It is important that personal information is not accidentally lost or revealed to anyone who does not have a right to see it.

It is vital that you do not save any personal data onto your home computer and that you ensure that no-one else in your household is able to access any information. You must have up-to-date anti-virus software installed and ensure you apply all security updates to your computer operating system. If you need to print something out when you are at home you should either shred it afterwards (if you are able) or bring it back to work for shredding.

If at all possible avoid taking personal data home. It is better to put it somewhere that can be accessed from home without having to be physically carried there in paper form or on a disk or memory stick. Consider finding a way to anonymise information that you need, to encrypt it or password protect it.

If you regularly need to take personal information home then you should have a system to record what information you take, when it was taken, why, and when it will be brought back. This means you can be sure that you know where all of your information is. For academic staff, your Course Support Officer may be able to help with this, for other staff you should consult your line manager.

Privacy Notices

When collecting personal data, staff should consider whether or not a privacy notice needs to be included. This is the oral or written statement that individuals are given when information about them is collected. It is often entitled 'fair processing notice' or a more accessible title would be 'how we use your information'.

In general terms, a privacy notice should state:

- our identity;
- the purpose or purposes for collecting the information;
- the categories of personal data concerned;
- the period for which the data will be stored;
- any extra information you need to give individuals in the circumstances to enable you to process the information fairly (e.g. with whom the information will be shared).

When deciding whether to use a privacy notice and how to phrase it, try to put yourself in the position of the people you are collecting information about. Ask yourself:

- do they already know who is collecting the information and what it will be used for?

- is there anything they would find deceptive, misleading, unexpected or objectionable?
- are the consequences of providing the information, or not providing it, clear to them?

You should take into account the consent already received from students as part of their enrolment at Central and you may also wish to include a link to the data protection section of MyCentral.

Privacy notices help Central to comply with the data protection principle of processing personal data fairly and lawfully. The School has a standard template for such documents, and if you have any questions about this (or other data protection matters) please contact the Data Protection Officer.

Section 6: Data Subject Rights

The General Data Protection Legislation gives all 'data subjects' – including staff, students, and alumni – particular rights with respect to how their personal information is collected, stored and processed by the School.

The following provides an overview of those rights, and how they are addressed by Central. Further details can be provided by the Data Protection Officer upon request (dataprotection@cssd.ac.uk).

Right to be informed

Individuals have the right to be informed about the collection and use of their personal data. Central accordingly publishes privacy notices for those groups whose information it collects: there are separate privacy notices for students, staff, alumni, donors, job applicants, short courses participants, and for the website. See Section 5 for further information.

Rights of Access, Data Portability and Erasure

Individuals have the right to obtain access to their personal data, known as a Subject Access Request. Thus an individual who makes a written request is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the data in a commonly used and machine readable format;
- given details of the source of the data (where this is available).

Some types of personal data are ***exempt*** from the right of subject access and so cannot be obtained by making a subject access request (e.g. data used for the prevention of crime).

Personal data will be provided to individuals in a secure manner, with 7zip software used to password-protect the information and the password provided to the individual separately.

Individuals also have a right to have personal data erased, known as 'the right to be forgotten'. This is not an absolute right and only applies in certain circumstances. The School keeps some personal information permanently, for statutory or archival purposes – for example, the academic records of its students. See the records retention schedules later in this document for more information.

A template for Subject Access Requests can be found in the appendices. Requests relating to the erasure of personal data should be directed to the Data Protection Officer at dataprotection@cssd.ac.uk.

In most cases an organisation must respond to a subject access request or a request for the erasure of personal data promptly and in any event within **one month** of receiving it.

What do I do if I receive a request?

If you receive a request for personal information, or for the erasure of personal data, you should always inform the Data Protection Officer as soon as possible. S/he will oversee the processing of all requests.

If you are asked by the Data Protection Officer to provide data about a student, please ensure that you cooperate as quickly and as efficiently as possible. We have to ensure that we respond within the statutory time limit.

Right to rectification

Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete. Details of how personal data can be corrected or updated, and the offices responsible, are provided in the relevant privacy notices.

Rights to restrict processing and to object

Individuals have the right to request the restriction or suppression of their personal data. As with the right to erasure (see above) this is not an absolute right and only applies in particular circumstances: for example, if the individual feels that their data has been unlawfully processed but does not wish it be erased.

Individuals also have the right to object to the processing of their data under certain circumstances: for example, where it is used for direct marketing purposes.

All requests relating to the processing of personal data are handled by the School's Data Protection Officer, by emailing dataprotection@cssd.ac.uk. Requests are responded to within one month of receipt.

Rights related to automated decision making

Central does not use any personal data for automated decision making, for example profiling.

Complaints

The School takes any complaints it receives about the use and security of personal information very seriously. Any complaints about the way in which Central handles personal data can be directed to the School's Data Protection Officer (by email at dataprotection@cssd.ac.uk or in writing to The Royal Central School of Speech and Drama, 62-64 Eton Avenue, London NW3 3HY).

Individuals can ultimately take any concerns that they have about Central's information rights practices to the Information Commissioner's Office: www.ico.org.uk.

Section 7: Data Breach Procedure

Introduction

Data breaches occur when personal information that is held by an organization is accidentally or deliberately lost, destroyed, altered, disclosed, or accessed. Unauthorised access to and circulation to a third party of data held on the School's student records system would constitute a data breach; so too would the loss of a laptop on which had been saved personal information relating to its staff or students.

The General Data Protection Regulation places an obligation on organisations to report data breaches to the Information Commissioner's Office ***within 72 hours*** of becoming aware of them, when it is determined that a breach poses a risk to individuals' rights and freedoms.

Further details can be found in Central's Information Security policy and guidance.

Procedure for reporting data breaches

If you suspect that a data breach has occurred, you should notify the Data Protection Officer ***immediately***, using the School's Data Breach Report Form and Activity Log (see appendices) to record briefly the nature of the breach, the data affected, and any actions that you took to resolve or contain the breach. The Data Protection Officer will then investigate the matter further, and make a decision about whether it is necessary to inform the Information Commissioner's Office and the data subjects concerned. All data breaches are reported to the Audit Committee.

Review of data breach procedures

All of Central's data protection-related procedures, including the one for reporting and resolving data breaches, are reviewed periodically, in the light of lessons learned from previous incidents or because of developments to guidance or best practice across the sector.

Section 8: Records Retention

This section sets out approved document retention periods in order that Central may:

- meet its statutory and legal responsibilities;
- meet its obligations to staff and students;
- comply with quality assurance requirements;
- reduce burdens on space and storage; and
- comply with data protection legislation by not retaining documentation longer than is justifiably necessary.

Notes:

1. Retention: Documentation may be retained for a longer period of time than stated in this document, but the department must make explicit the reasons for doing so (e.g. to retain project work that includes original data and/or analysis; for surveys of trends in student achievement; to use as examples to future students). The documentation must be destroyed when the stated purpose has been fulfilled.

2. Students: The policy on the retention of student work and files should be made available to students, via the data protection section of MyCentral.

3. Formats: Paper (e.g. files, forms, folders) or electronic (e.g. word processed documents, databases, spreadsheets, web, scanned images). Records held electronically must remain accessible and not lost in obsolete technology. Electronic storage should be reviewed periodically and, if necessary, arrangements made for it to be moved to new software. Long-term data should be held on a central server to ensure that it is adequately backed up.

4. Storage and Disposal: If it is helpful to retain both paper and electronic copies as the official record, this may be done; if not the non-official copy should be destroyed as soon as the need for reference ceases.

In order to make disposal easier, make a note on folders or folder lists when they are due for disposal at the creation or closure of that folder.

For each department, there should be someone with responsibility for organising disposal of specific files/data ('data weeding'), something that should be managed regularly, and no longer than once per year. Departments should review retention periods on an annual basis.

Paper documentation with personal data should be shredded on disposal.

6. Permanent Disposal: Before undertaking permanent disposal of student data it is vital to ensure that any student marks and results information, including pass lists, are retained by the Academic Records Office, or on the Student Records system. If in doubt, please check with the Academic Records Office (aro@cssd.ac.uk) before destroying files.

Records which may be routinely destroyed

As a rule, the following types of records have no significant operational, informational or evidential value. They can, therefore, be destroyed as soon as they have served their primary purpose.

- Announcements and notices of meetings and other events, and notifications of acceptance or apologies.
- Requests for stock information such as maps and travel directions, brochures, etc.
- Requests for, and confirmations of, reservations for internal services (e.g. meeting rooms) where no internal charges are made.
- Requests for, and confirmations of, reservations with third parties (e.g. travel, hotel accommodation, restaurants) when invoices have been received.
- Transmission documents: letters, fax cover sheets, email messages, compliments slips and similar items which accompany documents **but do not add any value to them**.
- Message slips.
- Superseded address lists, distribution lists etc.
- Duplicate documents such as:
    - 'CC' and 'FYI' copies;
    - drafts;
    - 'Snapshot' printouts or extracts from databases;
    - 'Day Files' (chronological copies of correspondence).
- Personal diaries, address books etc.
- Working papers, where the results have been written into an official document and which are not required to support it.
- Stocks of in-house publications which are obsolete, superseded or otherwise useless (e.g. magazines, marketing materials, prospectuses, catalogues, manuals, directories, forms, and other material produced for wide distribution).

Published or reference materials, internal or external, which require no action and are not needed for 'record' purposes (e.g. trade magazines, vendor catalogues, flyers, newsletters).

Academic Registry

Student Files

This includes files held by the Academic Records Office, the Course Support Office and the Student Advice Service. Files held by the Learning Centre are listed separately below.

Data / Document Type	Required Retention Period	Basis for retention period
Personal details	Permanent	Academic record kept permanently to enable production of transcripts/references
Progression details	Permanent	
Transcript details	Permanent	
Academic appeals	Last action on case + 6 years	Degree administration; future OIA reviews
Student Complaints	Last action on case + 6 years	Degree administration; future OIA reviews
Student Disciplinaries	Last action on case + 6 years	Degree administration, including production of references; future OIA reviews
Formative assessment records	Current academic year	Degree administration
Summative assessment records	Award Board confirmation + 6 months	Degree administration
Student academic feedback	Course completion + 6 years	For production of references
Mitigating circumstances	Current academic year + 1 year	Degree administration/ appeals
Examination Board papers	Current academic year + 6 year	Best practice; Exam Board minutes kept permanently
Registration records	End of registration + 6 years	Best practice
Transfers	End of registration + 6 years	Best practice
Withdrawals	End of registration + 6 years	Best practice
Terminations	End of registration + 6 years	Best practice
Admissions records – successful applicants	End of registration + 6 years	Best practice
Admissions records – unsuccessful candidates	Completion of admissions process + 1 year	Best practice

Quality Assurance Files

A. Quality and Standards

Data / Document Type	Required Retention Period	Basis for retention period
QAA HE Review/Institutional Audit/Collaborative Audit documentation - evidence	Electronic - permanent archive Paper - end of Review/ Audit year plus six years	Best practice
QAA HE Review/Institutional Audit/Collaborative Audit documentation - SED	Electronic - permanent archive End of Review/Audit year plus six years	Best practice
QAA HE Review/Institutional Audit/Collaborative Audit documentation – response to the results and follow up	Electronic - permanent archive Paper - end of Review/Audit year plus six years	Best practice
QA Handbook editions	Permanent archive – electronic	Best practice
Academic Regulations editions	Permanent archive – electronic	Best practice
Periodic Programme Review – documentation for panel	Permanent archive – electronic Paper - End of the current academic year plus six years	Best practice
Periodic Programme Review – report and response	Permanent archive – electronic	Best practice
Validation Report, Feasibility Study and other Panel supporting documentation	Paper - end of current academic year plus six years Minutes – permanent electronic archive	Best practice
Programme specifications	Permanent electronic archive – published on website	Best practice, and for the production of academic transcripts
Unit Outlines	Permanent electronic archive – published on website	Best practice, and for the production of academic transcripts
External Examiners reports and responses	Electronic permanent archive	Best practice
Appointment forms/CVs relating to selection and appointment of	End of appointment plus one year	Best practice. A permanent record of the basic details of External

External Examiners		Examiner appointments (name, institution, programme appointed to, appointment dates) is kept permanently
Expenses claim forms from External Examiners	End of the current tax year plus three tax years	Best practice
Annual monitoring of programmes	End of the current academic year plus six years	Best practice
All School committee minutes and supporting documentation	Electronic – permanent archive Paper - end of current academic year plus six years	Best practice
Sub-committee minutes and supporting documentation	Electronic – permanent archive Paper - end of current academic year plus six years	Best practice

B. Collaborative Provision

Data / Document Type	Required Retention Period	Basis for retention period
Collaborative Provision approval panel documentation	End of the current academic year plus six years	Best practice
Formal agreements with partner organisations (MoU/MoA)	Life of collaboration plus six years	Best practice
Register of collaborative provision	Permanent electronic archive	Best practice

Development and External Affairs

Includes all short course and non-credit-bearing student files, and alumni records.

Press & PR		**Basis for retention period**
Records of the organisation and administration of public events, campaigns and official visits	Permanent	Kept for reference, future planning and analysis
Media enquiries and responses provided	End of Employment + 3M (then review)	Kept in current Press and PR Manager's outlook files – to be passed to replacement as required, when files will be kept active for 3 months, then reviewed/ disposed of as necessary
Planning and organisation of media briefings and interviews	End of Employment + 3M (then review)	Kept in current Press and PR Manager's outlook files – to be passed to replacement as required, when files will be kept active for 3 months, then reviewed/ disposed of as necessary
Press releases, statements and distribution campaigns	Permanent	Kept on the Z: drive for reference, future planning and analysis
Monitoring and analysis of media coverage of Central, press cuttings	Permanent	Kept on the Z: drive for reference, future planning and analysis
Short Courses		
Creation and preservation of permanent short course student record on QLS	Permanent	In line with all QLS records
Short Course student registers both electronic and printed	By end of academic year following 5-yrs	Best practice
Excel data base with short course Diploma auditionee	By end of academic year following 5-yrs	Best Practice
Short Course waiting list – electronic	By end of academic year following 5-yrs	Best Practice
Youth Theatre hard copy & electronic emergency contact sheet	By end of academic year following 5-yrs	Best Practice
Short Courses receipt hardcopy	By end of academic year following 5-yrs	Best Practice
Auditionee feedback forms Diploma	By end of academic year following 5-yrs	Best Practice

DEA Marketing		
Marketing collateral, print and online including prospectus, advertisements, brochures, leaflets, show programmes, banners, posters, and promotional films	Permanent	For archival purposes
Student recruitment promotional materials	Permanent	For archival purposes
Photos in the image bank of shows, sessions/classes, festivals, events	Permanent	For archival purposes
Logos & branding	Permanent	For archival purposes
Student website profiles	3 academic years, including the year of graduation	To support students' continued promotion during transition period between graduation and professional career
Box office subscriber list	Permanent/until subscriber opts out	To enable marketing activity for Central's public productions
Alumni		
Alumni records administration (personal contact details and recorded contact with the School)	Permanent	Unless alumni asks that their records be removed
Alumni career news	Permanent	Best practice
Fundraising		
Fundraising campaign plans, promotional materials and event statistics	By end of academic year following 5-yrs (then review)	Informs the School's style and approach to fundraising events, provides a historical record of those involved, useful in analysing the strengths and weaknesses of a campaign. This is two years longer than the UCL Records Retention Schedule
Contact information for and notes about fundraising prospects	By end of academic year following 2-yrs	In-line with UCL Records Retention Schedule – the information is expected to be more or less up-to-date for this length of time
Business & Enterprise		

Email Enquiry	By end of academic year following 5-yrs (ongoing review)	Sales
Bought-in Data	Usually 1-yr	Sales
Training Enquiry Data Capture Form	By end of academic year following 5-yrs (ongoing review)	Sales
121 Training Enquiry Data Capture Form	By end of academic year following 5-yrs (ongoing review)	Sales
Open Course Booking Form	By end of academic year following 5-yrs (ongoing review)	Sales
Student Recruitment		
Marketing Campaign (operational plans)	By end of academic year following 3-yrs	To allow for effective evaluation year on year
Prospectus mailing lists	By end of academic year following 3-yrs	Prospective students plan so far in advance that this retention period would allow for a full cycle (inc gap year if applicable)
Event booking data and attendance monitoring forms	By end of academic year following 3-yrs	Prospective students plan so far in advance that this retention period would allow for a full cycle (inc gap year if applicable)
General student recruitment mailing lists	By end of academic year following 3-yrs	Prospective students plan so far in advance that this retention period would allow for a full cycle (inc gap year if applicable)
Online Advertising Campaign leads and associated data	By end of academic year following 3-yrs	To allow for communication with prospective students (leads) and effective evaluation of online advertising campaigns year on year
Website traffic analytical data	By end of academic year following 2-yrs	To allow for effective year on year evaluation of performance of website and its ability to provide users with a good experience
Course of interest student recruitment email marketing subscriber lists	By end of academic year following 3-yrs	Providing key info on relevant open days and other aspects of prospective students' course of interest at Central. Prospective

		students plan so far in advance that this retention period would allow for a full cycle (inc gap year if applicable)
Outreach-Placements		
Placement Confirmation Spreadsheet	By end of academic year following 5-yrs	HESA and QAA reporting
Placement Feedback Spreadsheet	By end of academic year following 5-yrs	HESA and QAA reporting
Outreach participant feedback report	By end of academic year following 5-yrs	OfS Reporting
Visiting Lecturer Information list	By end of academic year following 5-yrs	Quality Assurance
Student Ambassador Information Spreadsheet	By end of academic year following 5-yrs	OfS Reporting

Estates / Operations

Data / Document Type	Required Retention Period	Basis for retention period
Property access controls. Key registers, signing in logs, security logs.	2 Years	Statutory
Major building works. Project files, contract for building work, contractor review reports	End of works + 15 Years	Acts of Parliament 1980 c 58 s 14B(1)
Minor building works.	End of works + 6 years	Statutory
Statutory maintenance inspection and testing. Risk assessment and testing of items and systems including lifts, boilers, fire systems, alarms and water hygiene.	6 Years	Statutory
Statutory maintenance inspection and testing. Electrical testing and inspections.	5 Years	Statutory
Monitoring use/consumption of energy. Meter readings.	5 Years	Statutory
Waste management. Non-hazardous waste transfer notes.	2 Years	Statutory Instruments and EU Regulation 2011/988 reg 35(6)
Emissions management. Records associated with the CRC Energy Efficiency Scheme	Permanent	Statutory Instruments and EU Regulation 2010/768 art 57(3)

Finance

Financial records are bound by legal requirements within the Companies Act 2006 and the HMRC.

All records can be maintained in electronic mode or paper.

PURCHASE INVOICES AND SUPPLIER DOCUMENTATION	
Document type	**Required retention period**
Payments cash book or record of BACS/cheque payments	6 years
Purchase ledger	6 years
Invoice – revenue and expenditure	6 years
Invoice – capital item	10 years
Successful quotations for capital expenditure	Indefinitely
Petty cash records	7 years

INCOME/MONIES RECEIVED	
Document type	**Required retention period**
Bank paying in counterfoils	6 years
Bank statements	6 years
Receipts cash book	6 years
Sales ledger	6 years
Remittance advices	6 years
Bank reconciliations	6 years
Deeds of covenant	12 years
Legacies	6 years
Correspondence regarding donations	3 years

OTHER DOCUMENTS	
Document type	**Required retention period**
Investment certificates	Indefinitely
Investment ledger	Indefinitely
Fixed-assets register	Indefinitely
Agreements: With suppliers Leases Rental and HP Licensing agreements Indemnities and guarantees Loan agreements Other contracts and agreements	Under seal – 12 years after expiry Other – 6 years after expiry

Governing Body

Data / Document Type	Required Retention Period	Basis for retention period
Minutes of AGM, Governing Body & Committees	Permanent	Companies Act/Charities Act
Central's Company Registration Certificate	Permanent	Companies Act/Charities Act
RCSSD Articles of Association	Permanent	Companies Act/Charities Act
Royal Charter	Permanent	Companies Act/Charities Act
Central's Companies House returns	Permanent	Companies Act/Charities Act
Register of Interests – Central's Governing Body	6 years following end of office	OfS guidance
Governors E&D data	6 years following end of office	Central's Policy
Beatrice Lille Trust: Documents and Minutes	Permanent	Companies Act/Charities Act
CSSD Enterprises – Company Registration, Companies House returns & minutes	Permanent	Companies Act/Charities Act
• Contract with customers, suppliers or agents, • licensing agreements, • rental/ hire purchase agreements, • indemnities and guarantees • other agreements or contracts	*Current practice - permanent* Legal requirement: Six years after expiry or termination of the contract, or if the contract is executed as a deed, twelve years	*Central's Policy* Limitations Act
OfS annual returns	Permanent	*Central's Policy*
Audit reports	Permanent	Limitations Act
Legal Advice	Permanent	JISC

Phase 5

Data / Document Type	Required Retention Period	Basis for retention period
Initial Proposals		
End user requirements	6 years	Limitations Act
List of approved suppliers	Permanent – active	Limitations Act
Statements of interest	1 year	Limitations Act

Draft specifications	Once agreed	Limitations Act
Agreed specification	6 years from end of contract	Limitations Act
Evaluation criteria	6 years from end of contract	Limitations Act
Invitation to tender	6 years from end of contract	Limitations Act
Tendering		
Unsuccessful tender document	1 year	Limitations Act
Successful tender document	6 years from award of contract	Limitations Act
Background information	1 year	Limitations Act
Interview panel notes	1 year from end of contract	Limitations Act
Commissioning letter	1 year from end of contract	Limitations Act
Signed contract	6 years from end of contract *Permanent*	Limitations Act
Contract operation and monitoring		
Reports from contractors	2 years from end of contract	Limitations Act
Schedules of work	2 years from end of contract	Limitations Act
Bills of quantity (building contracts)	16 years	Limitations Act
Surveys and inspections	2 years from last report	Limitations Act
Records of complaints	6 years from end of contract	Limitations Act
Disputes over payment	6 years from end of contract	Limitations Act
Final accounts	6 years from end of contract	Limitations Act
Minutes and papers	*Current practice - Permanent* Legal: 6 years from end of contract	*Central's Policy* Limitations Act
Amendments to contracts		
Changes to requirements	6 years from end of contract	Limitations Act
Forms of variation	6 years from end of contract	Limitations Act
Extensions to contract	6 years from end of contract	Limitations Act

Human Resources

Data / Document Type	Required Retention Period	Basis for retention period
Appointment details (such as application form, monitoring form, authorisation to appoint, proof of eligibility to work in the UK, qualification certificates, employment references).	The information is held on file for the duration of their employment and up to 6 years after resignation. Employees' basic employment record (name, job title/role) is kept permanently.	To satisfy UK employment legislation such as Equality Act, UKBA regulations etc. To validate and confirm suitability/credentials for new role.
Personal details form which includes information the protected characteristics and bank details.	The information is held on file for the duration of their employment and up to 6 years after resignation.	To be able to make payment to staff in line with payroll requirements. To satisfy the requirements of the Equality Act 2010 and payroll information (Taxes Management Act 1970).
Contract of employment and conditions of service (such as Framework Agreement for the Pay and Conditions of Service for Staff, Terms and Conditions for hourly paid workers and contract variations).	The information is held on file for the duration of their employment and up to 6 years after resignation.	To verify employment references. To safeguard against employment tribunal cases. To comply with equal pay for work of equal value.
Employment history	The information is held on file for the duration of their employment and up to 6 years after resignation.	To verify salary and pay data. To verify employment references. To comply with Working Time Regulations 1998
Annual Leave	The information is held on file for the duration of their employment and up to 6 years after resignation.	To calculate holiday accrual calculations.
Sickness (health and wellbeing)	The information is held on file for the duration of their employment and up to 6 years after resignation.	To calculate and verify sick-leave entitlement and pay. To ensure compliance with the

		statutory sick pay regulations 2014. To comply with Health and Safety and Work Act 1974.
Reward & Recognition (including pension)	The information is held on file for the duration of their employment and up to 6 years after resignation. Individuals pension records – 12 years after the benefit ceases.	To ensure equal pay and work of equal value. To safeguard against employment tribunal cases.

IT

Data / Document Type	Required Retention Period	Basis for retention period
Initial development, modification and maintenance of IT systems	Life of system + 5Y	JISC
Systems development projects	Life of system + 5Y	JISC
Licensing	Life of system + 5Y	JISC
User requests for technical and application support, and reporting of problems	Resolution + 1Y	JISC
User account management	Expiry of account + 1Y	Good practice
Creating user name, password and e-mail account	Expiry of account + 1Y	Good practice

Learning Centre

Data / Document Type	Name	Required Retention Period	Basis for retention period
Form completed with student- Consent to share form, including disability details	'Consent to share' form ROCI (Release of Confidential Information form)	6 years	To facilitate support
Notes made and held on file- Disability/medical condition/SpLD details from **applicants**. Medical history and support required, including correspondence and emails.		1 year	To facilitate support
Notes made and held on file- Disability/medical condition/SpLD details from **current students**. Medical history and details of support required, including correspondence and emails	'IGRAS' – Internal Guidance Report for Academic Support	6 years	To facilitate support
Screening documentation, including test results and history, carried out within central together with the student.	'Dyslexia/SpLD Screening questionnaire'	6 years	To facilitate support
Documentation held on file – Medical evidence, ie. Doctors letter		6 years	To facilitate support
Documentation held on file – Diagnostic report (SpLD)		6 years	To facilitate support

Documentation held on file - Needs assessment report, carried out external Assessment centres, and held on file, detailing students disability/Specific Learning Difficulty and recommendations for support	'Needs assessment' 'Pre-assessment form' 'Booking form'		To facilitate support
Documentation held on file – Letters from Student Finance England, in relation to the Disabled Students Allowance (DSA), by email and paper copies held.	DSA application form 'DSA1' letter 'DSA2' letter	6 years	To facilitate support

Library

Data / Document Type	Required Retention Period	Basis for retention period
Library Services Collection Management Policy.	For the duration of the policy.	Sets out the collection, selection, retention and deletion policy of Library Services including The Archive.
Depositor and Donor Agreements.	Permanent.	Used in the event of collection re-evaluation when items may be withdrawn. It enables Library Services to identify the original donor and meet agreements.
Library Loans.	End of Registration plus one year.	Helps us build Library statistics and meet SCONUL requirements.
Registration of Users.	End of Registration plus one year. Information about debtors is kept indefinitely.	Helps us build Library statistics and meet SCONUL requirements.
Record of Inter-Library Loans.	End of Registration plus one year.	Helps us build Library statistics and meet SCONUL requirements.
Requests for Access to the Archive.	One Year	Helps us build Library statistics and meet SCONUL requirements.
Access to The Archive	Permanent.	Helps us build Library statistics.
Object Movement Records.	Permanent.	Helps us keep track of where and when collections have been loaned to external organisations.
Exhibition Records held by the Library Archive including Plans, Guides and Catalogues.	Permanent.	Builds a record of items appearing in exhibitions- when and where.
Conservation Records.	Permanent.	Builds a record of items conserved/preserved.

Research Office

	Data / Document Type	Required Retention Period	Basis for retention period
Admissions	AHRC Applications	6 years	Facilitate application process
	Applications Received Includes application form and some of the following: applicants' CV, emails, research proposal.	6 years	Facilitate application process
	Research Degree application forms	Indefinitely – subject to updating	Facilitate application process
	New students details and photos	6 years	Facilitate registration process
	Recruitment: PPT presentation	6 years	Advising potential applicants involves providing some information on leaver destination. Likely to be updated more frequently than 6 years.
	Reports of applications received	6 years	Facilitate application process
	Visiting Research Fellow and Scholar applications	6 years	Facilitate application process
	Spreadsheet: Admissions Correspondence	6 years	Recording applicants' expression of interest and applications
	Intent of study forms	6 years	Advising potential applicants
	Research proposals	6 years	Advising potential applicants
Current Students	PhD funding (scholarship applications)	To point of award	Facilitate application process
	Student files. Includes application form, scheme of work, supervision notes, upgrade materials, training and practice funds, suspension documents, research proposal	To point of award + 6 years	Facilitate the tracking of students' PhD work and milestones
	PhD topics	Permanent	Recording research areas
	RDC PHD Candidate List	To point of award	Tracking students' PhD work and milestones
	Awarded Students – PhD Examination	To point of award + 6 years	Exam information held post award to be

	Includes: Examination entry form, correspondence with examiners, examiners reports, thesis submitted for examination, thesis submitted after revisions		reduced to the requirements of UoL – namely the holding of final thesis.
	List of PhD Viva info Includes names of examiners and chairs for coming vivas	Permanent	To assist and record the organising of PhD Viva s
Alumni			
	Awarded Students – Student files. Includes: application form, scheme of work, supervision notes, upgrade materials, training and practice funds	To point of award + 6 years	Administration of the Degree
	Awarded Students – PhD Examination Includes: Examination entry form, correspondence with examiners, examiners reports, thesis submitted for examination, thesis submitted after revisions, award letter	To point of award + 6 years	Administration of the Degree
	Non-Awarded Students – Student files. Includes: application form, scheme of work, supervision notes, upgrade materials, training and practice funds, withdrawal form, correspondence	To point of award + 6 years	Administration of the Degree
	Student Issues (Confidential) Includes reports to the Research Ethics Committee, and correspondence and documents on various sensitive issues	6 years	Or as advised – to ensure information is available for external investigations if appropriate
Exchange	Visiting Research application form	6 years	Facilitating applications
	Visiting Researchers' Reports (includes photos of work presented/made)	Permanent	Recording and advertising research activities

Technical Support Department

Data / Document Type	Required Retention Period	Basis for retention period
Video: BA ACTING / DATE / TP ASSESSMENTS & PRESENTATIONS	3Y	Academic challenge of grade etc
Video: MA COURSES & MFA ASSESSMENTS & PRESENTATIONS	2Y	Academic challenge of grade etc
Video: RESEARCH EVENTS and CONFERENCES	HELD UNTIL OTHERWISE NOTIFIED	Archive
Video: STAFF RESEARCH	HELD UNTIL OTHERWISE NOTIFIED	Archive
Video: MA ACTING FOR SCREEN Showcase Films	HELD UNTIL OTHERWISE NOTIFIED	Archive
Video: PERFORMANCES and SHOWINGS	HELD UNTIL OTHERWISE NOTIFIED	Archive
PAT certificates	5 years	Assurance
Inspection records	10 years	Assurance and in case of legal redress
RAMS (Risk Assessments/Method Statements)	As long as the activity is valid	Legal requirement MHSWR

TSD Technical

Data / Document Type	Required Retention Period	Basis for retention period
Sign offs. Genie, ladders, PAT, Harness	Student duration	Assurance
RAMS	As long as the activity is valid	Legal requirement MHSWR
Rescue plans	As long as the activity is valid	Assurance WAH regs
PAT certificates	5 years	Assurance
Inspection records	10 years	Assurance and in case of legal redress

TSD Workshop

Data / Document Type	Required Retention Period	Basis for retention period
PAT records	Life of tool	Regularly updated and monitored for safe use
COSHH records and MSDS from manufacturers	Duration of use of substance	Regularly monitored and referred to for safe use
Incident Reports/First Aid reports	Until investigation is completed or declared closed	Communication with HR and tutors, improving practices to reduce accidents
Induction Records	3 years or Graduation	Compliance, Monitoring
Risk Assessments	Life of Tool/Duration of Practice or physical hazard	HSE compliance, KPI, monitoring and reference
Old Drawings, drafting	Permanent or until replaced with a better version	Drawings of space, what will fit in space, and personal records for how things were made just useful
Warranty Information	Life of Tool	In case it breaks due to a manufacturer's defect
Tool, COSHH, material inventories and price lists	Permanent	Continually used and referred to
Induction plans and Pre-Use Checks	Permanent	Continually used, printed and referred to

TSD Wardrobe

Data / Document Type	Required Retention Period	Basis for retention period
Documentation of skills inductions		Good practice
Equipment maintenance information		Good practice
Actor's photos	As long as student is enrolled	Good practice
Actors measurements	As long as student is enrolled	Good practice
RAMS	As long as the activity is valid	Legal requirement MHSWR

Head of TSD

Data / Document Type	Required Retention Period	Basis for retention period
CDM Documentation per show	3 years	Legal requirement
Past and Current show budgets, including Visiting Professional expenditure	As long as felt valid	For setting of future budgets etc

Provision of Service Agreements	As long as felt valid	In case of disagreement and claim
Phase 5 drawings and meeting minutes	As long as felt valid	Assurance and in case of legal redress
RAMS	As long as the activity is valid	Legal requirement MHSWR

Appendices

Appendix 1: Subject Access Request Form

ROYAL CENTRAL
SCHOOL OF SPEECH & DRAMA
UNIVERSITY OF LONDON

Subject Access Request Form

If you wish to access personal information held about yourself by The Royal Central School of Speech and Drama, you should complete this form and return it to the Data Protection Officer. If you are acting on behalf of somebody else, we will additionally require written consent from the data subject before we release the information to you on their behalf.

The School will aim to comply with all requests for personal information as quickly as possible, and in any case within one month of receipt.

Please complete this form in block capitals or type

1. Details of the person requesting the information

Surname: Click or tap here to enter text. Forename(s): Click or tap here to enter text.

Address: Click or tap here to enter text.

Postcode: Click or tap here to enter text.

Telephone Number: Click or tap here to enter text. Email: Click or tap here to enter text.

2. Are you the data subject (i.e. the individual to whom the information that is being requested relates)?

Please select the appropriate box:

Yes: ☐ (Please go to question 4) No: ☐ (Please complete question 3)

3. Details of the data subject

Surname: Click or tap here to enter text. Forename(s): Click or tap here to enter text.

Address: Click or tap here to enter text.

Postcode: Click or tap here to enter text.

Telephone Number: Click or tap here to enter text. Email: Click or tap here to enter text.

What is your relationship to the data subject?: Click or tap here to enter text.

4. Details of specific information requested

If you would like to see specific documents, please describe these in as much detail as possible (including any relevant identifying information, such as dates and the department(s) in which the documents might be located):

Click or tap here to enter text.

5. General search

If you want a general search for personal information about you to be conducted, please indicate below which departments you would like to be searched for relevant data. Please also state your relationship to the School (e.g. current or former student or member of staff) to assist us in locating any data that we hold about you.

Relationship to School: Click or tap here to enter text.

Department	Search	Department	Search
Academic Records Office		IT Services	
Academic Registry		Learning Centre	
Admissions and Student Recruitment Office		Library	
Alumni Office		Marketing	
Business and Enterprise Office		Partnerships and Outreach Office	
Counselling Service		Placements Office	
Course Support Office		Press and PR Office	
Development (including fundraising)		Principal's Office	
Facilities and Estates		Research Services	
Faculty (i.e. academic programmes)		Short Courses	
Finance		Student Advice Service	
Human Resources		Technical Services	

Other (please specify): Click or tap here to enter text.

6. Declaration

I certify that the information provided on this application form is correct. I understand that I will be required to provide evidence of my identity, and that of the data subject if it is different. I also understand that it might be necessary to supply more detailed information about my relationship to the School and about my request.

I include with this request the following documentation:

For data subjects	Evidence of own identity.*
For those acting on behalf of data subjects	Evidence of own identity.* Evidence of the data subject's identity.* Written authority from the data subject to act on their behalf.

(* We require two forms of identification per person, including at least one with the individual's photograph and signature – for example, a driving license or passport ID page. Please do not send original documents to us by post.)

Data protection

The Royal Central School of Speech and Drama will use the personal information you provide to process your request, and to review our handling of your request if we are required to do so. Central will not share your personal information with third parties without your permission, or unless we are required to do so by law. For further information, please see our Data Protection Handbook at: https://www.cssd.ac.uk/content/data-protection-privacy.

Signed: Date: Click or tap here to enter text.

The completed form, and accompanying documentation, should be returned by post or email to:

The Data Protection Officer
The Royal Central School of Speech and Drama
62-64 Eton Avenue
London
NW3 3HY

Email: dataprotection@cssd.ac.uk

Appendix 2: Data Breach Report Form

ROYAL CENTRAL

SCHOOL OF SPEECH & DRAMA • UNIVERSITY OF LONDON

DATA BREACH REPORT FORM AND ACTIVITY LOG

Please report any data breaches promptly, and no later than the day on which the breach is discovered to have taken place. You should complete Section 1 of this form and email it to the School's Data Protection Officer at dataprotection@cssd.ac.uk.

Section 1: Initial Notification of Breach	To be completed by the individual reporting the breach
Date of breach:	
Date of discovery of breach (if different):	
Brief description of the data affected:	
Data subjects affected:	
Brief description of the incident, including how the breach occurred:	
Actions taken to resolve or contain the breach:	
Any other relevant details:	
Name and contact details (email / telephone number) of individual reporting the breach:	
For use by the Data Protection Officer or Deputy Data Protection Officer	
Received by:	
Date received:	
Investigation Lead:	
Date form sent to Investigation Lead:	

Section 2: Investigation Outcome	To be completed by the Investigation Lead and/or the Data Protection Officer
Summary of activity (including details of how the breach occurred):	
Measures taken to address or mitigate the breach:	
Follow-up actions (including any lessons learned):	
Training needs identified:	
Date outcome reported to Data Protection Officer:	
For use by the Data Protection Officer or Deputy Data Protection Officer	
Notification to ICO:	Yes/No If yes, notified on: If no, rationale:
Notification to data subject(s):	Yes/No If yes, notified on: If no, rationale:
Notification to other stakeholders:	Yes/No If yes, details and date: If no, rationale:
Date of notification to Audit Committee	

Section 3: Activity Log				
Date:	Time:	Action type:	Description:	User:

Appendix 3: Contents of Human Resources files (staff)

Human Resources files for Central employees are created in the Human Resources Department upon recruitment. The information may be held electronically and / or hard copy.

Human Resources files contain information relating to:

- Appointment details (including qualifications)
- Personal Details e.g. age, gender, medical information, disability, ethnicity, nationality
- Contract of Employment
- Conditions of Service
- Career History
- Leave e.g. annual, special, parental
- Wellbeing e.g. appropriate risk assessments, absence information, medication information
- Reward & Recognition
- Staff Development activities
- General Correspondence involving Human Resources e.g. salary progression, remuneration

Access to the Human Resources file is limited to:

- Members of the Human Resources department
- The employee
- The employee's current Line Manager, Head of Department, Director and Principal (or nominated representative).
- The employee's new Line Manager, Head of Department, Director and Principal (or nominated representative), in cases of transfer (after the offer has been made and accepted).
- A responsible person authorised by the Director of Operations for a specific and necessary purpose. (Where the Chair of a selection panel requests a personal file, this may be provided at the discretion of the Director of Operations, for the sight of the Chair only. It may be appropriate to provide only information from the file which is relevant to the selection process).

Appendix 4: Contents of Academic Registry files (students)

Principles

- Individual student files retained by the Academic Registry should be the sole definitive record of information provided by the student relevant to his or her enrolment as a student and of formal correspondence between the student and the School in relation to status as an enrolled student, withdrawal or completion date, and final attainment.

- The file will NOT include routine correspondence in relation to the student's work or day to day course activities except where these include – even at a very early warning level – indications of how the student's attainment, behaviour, health or fee status might affect his or her continuance on the course.

- The student file will NOT replicate all the information on the computer-based student record system. In particular, the record system is the definitive source of information about the student's address, other contact details, and current enrolment status.

- The Academic Registry's role in relation to the student file is to set it up, maintain it, and thereby ensure that, in the event of query or dispute, all the relevant form communications can be accessed in one place. It is not the role of the Academic Registry routinely to copy correspondence which has originated elsewhere to staff who may have an interest in it.

- The Academic Registry will not release information from the student file to other School staff below the level of the Executive Management Group unless the member of staff's role in relation to the student is clear, and the purpose for information is to be used is compatible with data protection legislation and with the School's duty of care to student.

- All information in the student file except the enrolment form and transcript will be destroyed 6 years after the student has left, unless consideration of any dispute, complaint or appeal has extended significantly beyond the student's leaving date.

Contents of the Academic Registry Student File

- Application form
- Enrolment Form
- Form recording payment plan and acceptance of regulations
- Letter (e.g. from LEA) recording eligibility for tuition fee support
- Copy of any overdue fee reminder letter from Finance, setting a deadline.
- Copies of all correspondence relating to special arrangements for fee payment, including exceptional deadlines or instalment plans
- Any AP(E)L form considered
- Course transfer form where applicable
- Withdrawal forms

- Deregistration letters
- Reregistration letters
- Correspondence relating to interruption of studies and dates for return
- A note from the Academic Registrar recording the fact that the student has made an appeal, or a complaint. (The full correspondence relating to the appeal or complaint would remain separate)
- A note from the Academic Registrar recording any sustained allegation of cheating or plagiarism (but details of the investigation would be held separately).
- A copy of any warning letter from the Academic Registrar or other senior member of staff.
- A copy of an exclusion letter sent by the Principal.
- A statement (provided by the relevant authority, via the Academic Registry) recording the fact that a letter has been sent under the Disciplinary Procedure, and where that letter is held if the letter itself is considered too sensitive for inclusion in the student file.
- A copy of any reference written for the student, showing the date when it was written.
- Transcript (currently when produced on request, eventually for all students)
- A copy of any form approving alternative assessment arrangements.

Procedures

- Academic Registry staff will create student files within one month of completion of enrolment. Individual files will initial consist of the application form, enrolment form, finance/regulations acceptance form.
- Files will be organised by course within start year for all current students.
- If a student transfers from one course to another, or defers from one cohort to the next, Academic Registry will move the file to the relevant course and entry year.
- Formal correspondence as defined above will be copied to the Academic Registry for inclusion on the student file. Academic Staff, Finance staff and Learning Centre staff will receive guidance on what should be copied to the student file, and when. For regularly occurring types of correspondence (e.g. fee warning letters) guidance will also specify who should receive copies or lists of recipients of a standard letter.
- Files remain organised by course within year, and held in Academic Registry, whilst the students remain on course.
- If a student permanently withdraws, or is permanently excluded, or is not permitted to progress on grounds of failure, the removal of the file from the cohort group will not be a priority (since all these facts are on the student record system). Academic Registry staff will mark the file (coloured sticker) to indicate that the student has left before completion.
- When the students have completed or left, the files remain in course-within-year order in the Academic Registry archive for six years.
- Six years after the students have left, Academic Registry staff remove from the files all except the enrolment form and transcript, and file the remaining documents alphabetically, without regard for course or start date. In this form they remain in the Academic Registry archive.

Course leaders currently also hold student files which contain correspondence and assessment information.

The following information is held by the Student Advice Service in relation to the Counselling Service:

- Total of previous year(s) sessions.

- Sessions this year: [Attended] [Phone or email] [Missed or no prior cancel] [Cancelled].

- Number of sessions by month: [Sept, Oct ….].

- Total number of sessions to date (includes missed, but not cancelled):
  [1] [2-3] [4-7] [8-15] [16+].

- Issue categories at first presentation – max of 4 (based on AUCC guidelines): [Abuse] [Academic: general] [Academic: dyslexia] [Academic: study skills] [Anxiety: general] [Anxiety: PTSD] [Addictive behaviours] [Depression and mood change] [Loss: bereavement] [Loss: separation/divorce] [Loss: other] [Other mental health: general] [Other mental health: body image disorder] [Other mental health: obsessive-compulsive] [Physical health: illness] [Physical Health: disability] [Eating disorders] [Relationships: general] [Relationships: welfare of other] [Self & identity: confidence] [Self & identity: meaning/spirit] [Self & identity: sexuality] [Sexual: general] [Sexual: health] [Sexual: pregnancy / termination] [Transitions] [Welfare & employment related] [Self harm] [Other].

- Severity rating at presentation: [Functioning well] [Intermittent concern] [Limited but negative impact] [One significant area of anxiety] [Several areas of distress] [All areas of coping limited] [Extreme difficulty in all areas] [Overwhelm].

Appendix 5: Contents of Learning Centre files

For monitoring of the effectiveness of the Service and for equal opportunities monitoring, as required at present and as will be likely for the future, the Learning Centre has devised a common monitoring profile for all student clients.

Information to be held on students and used for monitoring purposes is therefore specified below.

A. Common student information

- Academic Year (runs from 1 Sept to 31 Aug)
- Service reference code (initials plus date of first appointment)
- Course and year group (for ease of recognition rather than annual statistics)
- [Current student] [Prospective student] [Staff]
- [Foundation] [Undergraduate] [Postgraduate]
- [Full-time] [Part-time]
- [Home] [EU] [Overseas]
- Totally self-financing course: [Yes] [No]
- New contact this academic year: [Yes] [No]
- Referred by: [Self] [Tutor or other staff] [Friend or other students]

B. Equal Opportunities Monitoring (common)

- Gender: [Male] [Female] [Transgender].
- Sexual Orientation: [Heterosexual] [Lesbian / gay / bisexua] [Undisclosed / unknown].
- Age group this year: [under 21] [21-24] [25 or over].
- Marital Status: [Single] [Married / partnered] [Separated / divorced / widowed] [Undisclosed unknown].
- Race: [White: British / Irish / Other White] [Mixed: White & Black Caribbean / White & Black African / White & Asian][Asian or Asian British: Indian / Pakistani / Bangladeshi / Other Asian][Black or Black British: Black Caribbean / Black African / Other Black] [Chinese or other ethnic group: Chinese / Other ethnic]
- Disability: [Yes] [No] [Don't know] If yes: [Physical] [Learning] [Mental health] [Other / medical].

Appendix 6: Writing References for Students and Former Students

Key Facts and Principles

In writing references, we have a duty of care to the subject of the reference and also a duty of care to the recipient of the reference.

This means that either the School or the individual writing a reference could be open to legal challenges on grounds of negligence, misrepresentation or defamation. For example, the subject of a reference could claim damages if he or she is unsuccessful in an employment application for which a reference has expressed unfavourable opinion which cannot be substantiated by verifiable facts. An employer could claim damages if material information was not disclosed.

Under data protection legislation, the subject of a reference cannot demand access to the reference from the provider of the reference. Data subjects can ask the recipient of a reference to disclose it. The recipient has a duty of care to the writer, as well as to the subject, and can refuse to do so. Some institutions advise reference-writers to make it explicit in the reference if they are unwilling for the content to be disclosed to the subject. Even if a reference is marked confidential, there may be an obligation to disclose it if required to do so by a court, or when defending a claim for damages.

General Guidance

- Stick to the facts as far as possible. Check the facts and do not rely on memory and personal impressions. The facts should, as far as possible, be verifiable from information on the student's file or on the student record system.
- Phrase references so that the facts are clearly differentiated from opinion.
- Opinions given should be with consistent with the student's achievement to date. For example, it is possible to express an opinion about the likely degree classification of a student who has not yet graduated, on the basis of academic judgement and performance to date, but any such opinion should accord with the record of results to date. (There has been a court case following the withdrawal of a job offer on the basis of prediction that a student's classification would be lower than that actually achieved, in which it was found that the opinion did not accord with evidence available at the time.) If, for example, a reference asks for comment on ability to meet deadlines, and there is a record of penalties for late submission of work, a negative opinion can reasonably be given.
- A reference for a student who has completed should be updated to replace any predicted results with actual results. This may be done even if the original author of the reference is no longer on the staff of the School.
- Opinions should be within the referee's area of professional competence. For example, opinions about the possible impact of medical circumstances should not be given by a referee not competent to judge these.
- Do not use ambiguous wording in an attempt to disguise a poor opinion. Avoid wording which effectively invites the recipient to "read between the lines".
- If you have a firm opinion, based on facts, relevant to the reference, state it in words which make it clear beyond doubt that it is an opinion. ("I believe that X is well-suited

to the post" is better than "X will be a great success in the post"). Less definite opinions, based on unverified impressions, should not be aired or hinted at.

- Do not provide any reference which includes opinion more than three years after the student has left the course. At this stage, confine any reference to factual information about period of study and results achieved.
- Do not, unless unavoidable, give telephone (or other oral) references. These can be open to misinterpretation, or to unconscious "filtering" as the message is reported at the recipient end. If it is necessary to give an oral reference, or if it is clearly in the interest of the subject to do so, be particularly careful to confine yourself to the facts, make a written note of what you have said, and follow up the conversation in writing.

Good Practice

- As far as possible, write references which you would be able to show to the subject, and which the subject would be likely to consider fair, even if critical.
- If writing anything other than a standard good reference, check it with another member of staff who has worked with the individual who is the subject of the reference.
- Include in the reference your role/job title at the School and your relationship to the subject of the reference.
- All references should be marked "confidential". However, the data subject may ask the recipient for a copy. Some receiving organisations will ask permission, but they are not required to do so. If you explicitly do NOT want the subject to see the reference, you should make this clear. You could head the reference "private and confidential – for the attention of the addressee or selection panel only", or you could include the phrase "I do not consent to this reference being shown to the person it concerns".
- Include, at the end of the reference, the sentence "This reference is provided in good faith, but the School does not accept any liability in the respect of the accuracy or completeness of the statements contained in it."

Dealing with specific difficulties

Sensitive information:
A disability should be mentioned if it seems likely that it will have a material effect on the subject's capacity to undertake the employment or course for which the reference is sought, but otherwise not. For full compliance with data protection legislation, the subject of the reference should give consent before disability information is included.

If a student is or has been in bad standing with the School (e.g. financial, or disciplinary) this should normally not be mentioned unless you consider it directly relevant to the duty of care owed to the recipient of the reference. Any form of misconduct which has already been penalised (e.g. plagiarism) should not normally be mentioned in a reference. Discuss the issue with the Academic Registrar before sending the reference.

Spent convictions:
Details of convictions deemed to be "spent" under the Rehabilitation of Offenders Act of 1974 should not be mentioned in a reference. If the student is entering an area of employment for which all convictions must be disclosed, the onus of responsibility to secure a criminal record disclosure rests with the employer or educational provider. If explicitly

asked, however, a reference may confirm that a criminal record disclosure has been received and that no convictions were found.

You do not know the subject of the reference/you do not have information requested:
Do not give opinions, unless they are directly attributed to a colleague or former colleague who knew the student. If you know nothing about (for example) the subject's honesty and integrity, make this clear. You can use wording like "I know of nothing that would lead me to question his honesty".

The student left without explanation, or was deregistered for non-payment:
Stick to the facts that the student attended between (dates) and left in (month year) having (successfully) completed such and such (or n years of a course lasting n+ years). Do not speculate about the underlying issues.

Procedures

- References for students and past students may be written by Course Leaders or designated members of the course team who know the student.
- For students still enrolled at the School, and for up to three years after a student has left, the reference will be held on file by the Academic Registry. If the members of staff who prepared the reference has left, or does not wish to tailor the reference to the specific enquiry, the reference may be sent out, in a form which includes appropriately expressed opinion, by the Academic Registry, with a pre-printed note to the effect that it was written at the date shown, and concerns the subject as at that date.
- A copy of any standard reference prepared for general use should be placed on the Academic Registry student file, where it may remain for six years, after which it will be destroyed.
- More than three years after a student has left the School, a standard factual statement of the student's period of study and qualification awarded will be issued, by the Academic Registry.
- Individual members of the academic staff who have retained contact with students may provide personal references more than three years after students have left, but do so at their own risk, must not use the School's letter head, and must make it clear that the write in a personal capacity.
- Academic Registry staff are responsible for the information held on the student file. Other staff – particularly academic staff – may have reason to access it. Academic Registry staff will normally ask the purpose for which information on file is sought, especially in the case of students who have left the School. If a sound reason for requiring access (within policies on data protection) is not given, information from the files may not be released without authorisation from am member of the Executive Management Group.

Challenges and Liability
If you are challenged over a reference you have written, do not enter into discussion or admit liability. Refer the matter immediately to the Dean of School.

Appendix 7: Writing References for Staff Members

Procedures

The issuing of all staff references, whether past or present, is centralised within the Human Resources department. Therefore all staff reference requests should be forwarded to the Human Resources department for official response.

It is important that with any response consistency is maintained. The Human Resources department will liaise with the named referee, as appropriate, for their contribution to the reference on matters relating to character and ability. The reference will be signed and issued by the Human Resources department but will state where a contribution has been made to the reference by the named referee.

The official response will be issued by the Human Resources department on Central headed paper.

General Information

There is no legal obligation on an employer to provide a reference in respect of an ex-employee unless an obligation to do so is included in the contract of employment. However, there may be a regulatory obligation as certain industry bodies require a reference to be provided (e.g. the PIA, now part of the Financial Service Authority).

If a reference is given, great care needs to be taken in its preparation. The employer owes a duty of care in negligence not only to the person who is the subject of the reference, but also to the recipient of it. It should also be noted that there may be claims for discrimination if the employer refuses to provide a reference on grounds of sex, race or disability or because the particular employee has brought a claim for discrimination against the employer (see below).

Ensuring accuracy of references

It is the duty of the reference writer to exercise reasonable care and skill in providing a reference. The writer should take reasonable steps to:

- ascertain that the information on which the reference is based is factually correct;
- express opinions (if the writer chooses to do so) about the subject of the reference which are reasonable in the circumstances and can be justified; and
- create a fair impression overall. This might mean putting certain factual matters into context where not to do so would create a misleading impression.
- Having checked the factual accuracy of statements and the reasonableness of opinions contained in the reference, the reference writer should then “stand back” and ensure that the effect of the whole is fair and not misleading. If stating certain

facts, without more, might be misleading, then the writer should elaborate matters further.

- A reference writer who is negligent in the above respect will render the employer liable for any loss which the employee or the recipient incurs as a direct result of inaccurate statements, opinions or impressions.

- Many employers include a disclaimer in any reference they give. In view of the Unfair Contract Terms Act 1977, there is some doubt as to whether these disclaimers would be effective to exclude liability. In order to be effective the disclaimer must be reasonable and this would be determined by reference to the circumstances in which the reference is given and to its content. Subject to the above, as far as trying to avoid liability to the employee is concerned, it is important to ensure that the employee's prior written agreement is obtained to a reference being given on this basis.

Data Protection Legislation

Under data protection legislation (which extends to computerized and manual data), individuals are not entitled to have access to any reference given by the provider of the reference. However, the individual will be able to apply to a new employer, or potential employer, for a copy of the reference provided by the existing or previous employer.

This is significant, not only in terms of the individual being able to adduce evidence for a possible claim of negligence or in relation to discrimination, but also under the legislation itself for the removal or correction of inaccurate data. The individual could use the right of access against the recipient of the reference and bring a claim against the provider. This is a major change in the law and leads to the anomalous position that an individual enjoys greater rights of access against the prospective employer than against the current employer. The legislation also enables an individual to bring a claim for damages for actual harm suffered as a result of inaccurate data being processed.

Because the legislation prohibits the use or disclosure of personal data without the individual's consent the reference writer should make sure that he has the individual's consent to provide the reference. This will usually be the case but not, for example, if the prospective employer has made a speculative inquiry on its own initiative. In either case, the reference writer should ask the employer requesting the reference to confirm that the employee has consented to the reference being given.

With regard to the School, consent to request references is attained on the current application form.

Equal Opportunities

The non-provision of a reference by an employer is capable of being an act of discrimination even where the employment relationship has terminated.

It is generally unlawful to discriminate on grounds of race, sex, disability or trade union membership or activity. It is specifically unlawful to instruct, procure, induce, comply with, or knowingly aid an act of unlawful discrimination.

In giving and acting upon references, care should be taken to avoid overt or covert, intentional or unintentional acts of unlawful discrimination. This is particularly the case where opinions not based on any 'objective evidence' are sought or offered on the suitability of applicants. Opinions should therefore be backed up by objective evidence.

For further information and advice, please contact the Human Resources department.