Strategies for improving the handling of Confidential Records and Information in Abia State College of Education (Technical), Arochukwu

CHIMEZIE UMUNNAKWE UCHECHI[1], A K. JIBRIL[2]
[1]Provost Office, Abia State College of Education (Technical) Arochukwu
[2]Department of Electrical/Electronic Technology, Abia State College of Education (Technical) Arochukwu

Abstract- This paper set out to determine how confidential records are leaked in Abia State College of Education (Technical) Arochukwu and provided improvement strategies. The paper adopted descriptive survey research design. The instrument for the study is a 25-item questionnaire. The questionnaire was validated by three experts and its reliability was found to be 0.83. Copies of the validated questionnaire were administered to 32 admin staff of the College. The data collected from the questionnaire was analysed. The result of the analysis revealed the strategies to be adopted to improve the handling of confidential records in Abia State College of Education (Technical) Arochukwu. Based on the findings of the study, the paper recommended among others that confidential records should not be release to friends without authorization from higher authority, confidential records should always be under lock and key, no officer should be allowed to post confidential record in any College social media platform, more harsh punishment should be mated to staff found guilty of unauthorized release of confidential record(s), there should be periodic capacity building training on confidential record keeping techniques and physical locations where confidential records are store most be highly secured.

Indexed Terms- Strategies, Information, Records, Confidential Records, Abia State College of Education (Technical) Arochukwu

I. INTRODUCTION

Educational institutions create, handle and keep variety of records for day to day operations. A record according to Indiana University (2012) is information or knowledge on a specific subject and preserved in a typed, written, or electronic format. University of Adelaide (2009) describes record as anything that provides tangible evidence of information or past events. Records are classified in different ways. Records can be tangible (physical) or electronic, confidential or non-confidential. Educational institutions handle different types of records such as administrative records, equipment and supplies records, budget and finance documents, facilities and properties records, safety and security records, revenue records, contract records, athletic records, recruitment records, personnel records, payroll records, health services records, bank records, legal records, historical records, curriculum and instruction records and student's records (University of Colorado, 2018). Some of these records or information are confidential in nature. Confidential records and information are those records and information that are not available to public except allow by the law. Examples of confidential records and information include but, not limited to reference letters, student records, personnel records, evaluations of performance, health records, grievance files, appeal files and payroll records (PIM, 2008). Other confidential records include Investigative reports concerning alleged misconduct, Garnishment orders and family court documents or orders (West Virginia, 2013).

Disclosure of confidential records and information are limited to those personnel that require them for their official duties as well as those related to individuals in case of personal information. Confidential records and information are sensitive and vital. They are therefore to be kept in a secured environment. United Republic of Tanzania (2013) stated that confidential files (personnel files) should be safeguarded against unauthorized access, copying, alteration, removal of documents, disclosure of contents. Confidential files should also be protected against loss or damage. In addition, all files connected with an employee are considered strictly confidential and should be maintained in a secured location that is separate from other records. Files containing confidential information

are to be kept in locked cabinets or drawers with limited access. If personnel files are stored electronically, access also must be secured and limited (National Pork Board, 2010).

Although section 1 of the Nigeria freedom of information Act of 2011 provides that every citizen whether adult or minor is entitled to have access to any records under the control of the government or any public institution, it should be noted that there are certain information such as personal information that are exempted from disclosure to public. Individuals seeking for information from public institutions are by the act are required to make their application in accordance with section 1. This implies that any information disclosed by the staff of public institution without due process is illegal and will attract punishment

To guard against disclosure of confidential records and information, Abia State College of Education (Technical) Arochukwu put in place several measures. Despite these measures, some staff discloses confidential records and information. Such disclosure affects smooth operation of the College on one hand and on the other spoil the reputation of the College. It is against this backdrop that the researchers set out to find ways or strategies of improving the handling of College confidential records and information.

II. PROBLEM STATEMENT/JUSTIFICATION

Records and Information are used in day to day administrative operations in Abia State College of Education (Technical) Arochukwu. Among them, there are some confidential records and information that need to be protected against disclosure, addition, alteration or removal by unauthorized persons. But it is a fact that there are some staff of the College that are in the habit of disclosing, replacing, adding, removing and mutilating confidential records and information despite some measure in place. This behaviour does not only hinder smooth administrative operations in the College, but also cause embarrassment in the public eyes. It is on this basis that the researcher set out to find the ways or strategies of improving the handling of records in Abia State College Education (Technical) Arochukwu.

III. OBJECTIVES OF THE STUDY

The general objective of the study is to determine the strategies for improving the handling of the College confidential records and information. But specifically, the study sought to determine how confidential records are:

1. secured
2. Disclosed to unauthorized persons
3. Removed or altered
4. can be more secured

IV. RESEARCH QUESTIONS

The following research questions were formulated to guide the study.

1. How confidential records are secured in the College?
2. How confidential records are disclosed to unauthorized persons?
3. How confidential records are removed or altered?
4. How can confidential records can be more secured?

V. LITERATURE REVIEW

This section present different types of records created, handle and stored by organizations. The section also presents how information is secured. Access and disclosure of confidential information were also presented.

Types of Records
A record according to Indiana University (2012) is information or knowledge on a specific subject and preserved in a typed, written, or electronic format. There are different types of records. The following are some types of records taken from Leichtag family foundation(2022):

Accounting and Corporate Tax Records: Accounting and corporate tax records include, but are not limited to: financial statements; ledgers; audit records; invoices and expense records; federal, state, and property tax returns; payroll; accounting procedures; gross receipts; customer records; purchases; etc.

Workplace Records: Workplace records include, but are not limited to Articles of Incorporation, bylaws, meeting minutes, deeds and titles, leases, policy

statements, contracts and agreements, patents and trademark records, etc.

Employment, Employee, and Payroll Records: Employment records include, but are not limited to job announcements and advertisements; employment applications, background investigations, resumes, and letters of recommendation of persons not hired; etc. Employee records include, but are not limited to employment applications, background investigations, resumes, and letters of recommendation of current and past employees, records relating to current and past employee's performance reviews and complaints, etc. Payroll records include, but are not limited to wage rate tables; salary history; current rate of pay; payroll deductions; time cards; W-2 and W-4 forms; bonuses; etc.

Bank Records : Bank records include, but are not limited to bank deposits; check copies; stop payment orders; bank statements; check signature authorizations; bank reconciliations; etc.

Legal Records: Legal records include, but are not limited to all contracts, legal records, statements, and correspondence, trademark and copyright registrations, patents, personal injury records and statements, press releases, public findings, etc.

Historical Records: Historical records are those that are no longer of use to the organisations, but by virtue of their age or research value may be of historical interest or significance to the organisations

Privacy, Confidentiality and other Limits on Access

University of Adelaide (2009) presented a material on privacy, confidentiality and other limits on access as follows:

Personal information - Many of the records held by the University contain personal information. Any information or opinion from which the identity of an individual can be ascertained is considered to be "personal information". This includes a person's name, address, date of birth, student/staff identification number, and other personal characteristics. The University has a responsibility to collect, manage, use

and disclose personal information in accordance with the prevailing community standards of best practice, respecting the privacy of the individual. Everyone handling University records needs to be familiar with and follow these standards, as encapsulated in the Privacy Policy and Management Plan - this will be particularly important if you work with student records or personnel files, which contain predominantly personal information.

Financial information - such as tax file numbers, bank account or credit card details. These are a form of personal information, but are also generally subject to specific confidentiality requirements under financial regulations.

Health related information - such as counseling notes or medical information. In addition to being a form of sensitive, personal information, they are subject to additional regulatory and professional confidentiality requirements.

Student related information - including grades, progress and enrolment details of current, past and prospective students (including those who are offered a place but ultimately do not attend the University).

Legally privileged documents - this would include communications between you and legal representatives (including the Legal and Risk Branch of the University) or advice you receive from your legal representatives.

Information requiring confidentiality to ensure intellectual property right protection - such as patentable information which is in the course of being protected.

Commercially sensitive information - such as information provided by an industry sponsor in the course of a specific research project, disclosed on the basis of "commercial in confidence". Commonly this material would be protected by way of a confidentiality agreement (or confidentiality clauses in the research funding contract).

Confidential by way of agreement - if the University has agreed to keep something confidential under a contract, then it must comply with that agreement. If

you are agreeing to keep something confidential, you should run the terms by a legal advisor, such as someone in Legal and Risk Branch. Note that if the terms of a contract itself are intended to be kept confidential, then a special process must be followed before the contract is signed, otherwise the document will not be protected from access under Freedom of Information.

Storage of Records

University of Adelaide (2009) stated that it is important to keep records in conditions that ensure they are protected, secure and accessible for as long as they are required to meet the business requirements and legal obligations of the University. These physical storage requirements will vary depending on:

Physical characteristics: Records will be in a variety of formats or media, which will require specific protective packaging and environmental conditions.

Sensitivity and security: All records need to be protected from unauthorised access and should not be left unattended or in vulnerable locations. Records which have additional sensitivity include, but are not limited to:

- Personal information about staff or students
- Student or staff grievances.
- Information that is either commercial in confidence or legal in confidence

Regardless of whether records are hardcopy or electronic, the following are recommended to ensure effective storage:

- Store records in a way that will protect them from unauthorized access or disclosure, especially records that are sensitive.
- Records that originate in a digital form should remain digital. For example MS Office documents should be saved into an Electronic Document and Records Management System (EDRMS). Content Manager is the University's EDRMS. Not printing digital records assists the University to meet its strategic goal to reduce paper use.
- Hardcopy files that are registered in Content Manager can be returned to Records Services when they are no longer required by you.

- Use common sense when working out what records to store in your working areas, versus more remote storage. If hardcopy records need to be consulted frequently, keep them within your office space. Files registered in Content Manager can be returned to Records Services when they are no longer required by you.
- Use the records disposal schedules to help prioritise records for storage. For instance, if records are only required to be stored for a short period of time (such as less than 2 years) then it may be more efficient to keep them on site until they can be destroyed. By contrast, records identified for permanent retention will require the highest standards of care to ensure their longevity.
- Standard email programs and shared network drives do not provide recordkeeping functionality such as full record metadata, access and security. Therefore these are not suitable to meet the University's obligations under the State Records Act.

Conditions for Access to Personnel Records
Human Resource Management (1999) stated as follows:
(1) Management Access to Personnel Files:
a. Management will be allowed access to these files strictly on a need-to-know basis. Only the information regarding an individual's job performance and skill qualification will be open for review.
b. The employee's designated Business Manager will also be allowed access, but only to the section of the personnel file that pertains to funding of the employee's position.

(2) Employee access to his/her personnel file:
a. Employees are permitted to gain access to their personnel file by either calling or writing the Human Resource Management Department for an appointment. An appointment will be scheduled at a mutually convenient time. Records that are considered to contain sensitive or confidential information, such as reference letters, etc., may be excluded from the inspection. All inspections must be conducted in the presence of a designated member of the Human Resource Management Department.
b. Employees may not at their own discretion, mark up, or in any way change any file material that they believe

is incomplete, inaccurate, or irrelevant. They may, however, place a written statement of disagreement in the file.

(3) External Request for Personnel File Information:

a. Any external source such as a person or agency/company who request information from an employee's personnel file must first receive written clearance from the employee before any data is released. Verification of employment requests for active employees or positive responses to legitimate credit source inquiries must also contain the employee's signature.

b. Job references requested for former employees are limited to employment dates, positions held, and job location such as department/laboratory worked, unless additional information is requested in writing and only after obtaining the written consent of the individual involved.

Conditions for Access to Employee Medical Records

All medical records are held in complete confidence, in separate files, and are secured at all times. Employees may view and make copies of all or any part of their own medical records. Exceptions may be made to cooperate with legal, safety, and medical officials who need specific employee information, but not without the knowledge of the individual involved. In accordance with Act 1036 of the 1990 Louisiana Legislative Session, employees have the right of access within seven (7) working days to records relating to his/her drug tests and any records relating to the results of relevant certification, review, or suspension/revocation-of-certification proceedings. All information, interviews, reports, statements, memoranda, or test results received by the Pennington Center are confidential communications and may not be used or received in evidence, obtained in discovery, or disclosed in any public or private proceedings, except in an administrative or disciplinary proceedings or hearing, or civil litigation where drug use by the tested individual is relevant.

Non-disclosure of Confidential Information
National Council of Nonprofit Associations (2004) stated that:
Any information that an employee learns about {Organization Name}, or its members or donors, as a result of working for {Organization Name} that is not otherwise publicly available constitutes confidential information. Employees may not disclose confidential information to anyone who is not employed by {Organization Name} or to other persons employed by {Organization Name} who do not need to know such information to assist in rendering services.

The protection of privileged and confidential information, including trade secrets, is vital to the interests and the success of {Organization Name}. The disclosure, distribution, electronic transmission or copying of {Organization Name}'s confidential information is prohibited. Such information includes, but is not limited to the following examples:

- Compensation data.
- Program and financial information, including information related to donors, and pending projects and proposals.

Employees are required to sign a non-disclosure agreement as a condition of employment. Any employee who discloses confidential {ORGANIZATION NAME} information will be subject to disciplinary action (including possible separation), even if he or she does not actually benefit from the disclosure of such information. Discussions involving sensitive information should always be held in confidential settings to safeguard the confidentiality of the information. Conversations regarding confidential information generally should not be conducted on cellular phones, or in elevators,restrooms, restaurants, or other places where conversations might be overheard

Guidelines to Protect Confidential Records and Information
The following guidelines according to PIM (2998) should be considered for confidential records:

- Access to the confidential records should be restricted only to those employees that require the records and information in the performance of their assigned duties.
- Include "confidential" in the header or footer or as a watermark or stamp for each document containing confidential records and information.

- Photocopying confidential reports on a coloured paper designated for that purpose, e.g., closed session minutes and agendas on blue paper.
- Keeping records in a secure location, such as in locked file cabinets, in locked rooms, or on a secure server. Cabinets should always be kept locked when not in use and located in a private/secure area, and access to the cabinets should be limited to authorized employees.
- Confidential records and information should be placed in a file folder, envelope, or other form of cover when out of the secure cabinet.When the record is not in use, it should be returned to the cabinet right away.
- Confidential records and information should never be left in an open area such as in an in-basket or on a desk. The record should be returned to the cabinet when not in use.
- Confidential records and information must be destroyed by secure shredding or by other secure data destruction methods.
- Confidential records and information should be stored separately from other similar records to support controlled access.
- For electronic records, store confidential records in separate directories or files, restrict access to these directories or files, and remove by secure deletion only.
- Computer screens should be positioned to prevent unauthorized viewing.
- Use passwords to protect confidential records and information and protect your passwords
- (see Password Guidelines).
- Shut down programs or use password protection on your computer when you leave your desk.
- Turn off your computer when leaving your desk for a long period of time.
- Shred drafts when they are no longer useful, and delete drafts from your computer.
- If you have confidential records on a notebook or laptop computer, ensure that either the documents themselves or the system are password protected. Do not leave your laptop in an easily accessible area where it could be stolen. Consider using data encryption for protected confidential records and information on portable devices.
- When travelling with confidential records, do not leave them unattended in vehicles, hotel or meeting rooms. Do not work with confidential records where others can see them.
- Do not remove Ontario Student Records from the school.
- If confidential records and information must be faxed, include a fax transmittal page with a confidentiality statement. Verify that the number on the screen is accurate before proceeding with the transmission, and confirm receipt of the documents.

VI. MATERIALS AND METHOD

The procedure for carrying out the study is presented under the following headings: design of the study, area of the study, population for the study, sample and sampling technique instrument for data collection, method of data collection and method of data analysis.

Design of the study
This study adopted descriptive survey research design. The design enabled researcher to collect information on the ways of improving the handling of confidential records and information in Abia State Colleges of education (Technical) Arochukwu.

Area and Population of the Study
The study was carried out in Abia State College of Education (Technical) Arochukwu. The population of the study consisted of 56 staff of Abia State College of Education (Technical) Arochukwu.

Sample and Sampling Technique
Proportionate sampling technique was used for the study. A sample size of 32 staff was drawn from the population of 56 staff from various schools and units using proportionate sampling technique.

Instrument for data collection
The study made use of structured questionnaire as instrument of the study. The questionnaire incorporated four point Likert scale. The questionnaire consisted of five sections; A, B, C, D and E. Section A sought information on respondents' personal data. Sections B, C, D and E elicited information from respondents on how confidential records and information are secured, disclosed to unauthorized persons, removed and altered as well as how they can be more secured. The questionnaire was validated by

three experts. The validated questionnaire was then subjected to reliability test. The result of the test indicated that the questionnaire has reliability index of 0.83 using Cronbach alpha statistic.

Method of Data Collection
The researchers handed over the copies of the developed questionnaire directly to the respondents in the College and then explained to them how to fill them. After one week, the researchers collect back the filled questionnaires from the respondents.

Method of Data Analysis

Mean and Standard deviation statistics were used for the analysis of the data collected from the questionnaire. Any item with mean cut off point of 2.5 or more represents a strategy for improving handling of confidential records. On the other hand, items with means less than 2.5 do not represent strategies for improving handling of confidential records.

VII. RESULTS

Research Question 1
How confidential records are secured in the College?

Table 1: Means and Standard Deviations of the responses of Admin Staff on how confidential Records are secured in the College
N= 32

S/N	Item Statement	$\overline{X}$	SD	Remark
1.	Most of the College confidential records are secured in a special room	3.06	0.88	Agree
2.	Most of the College confidential records are secure metal filling cabinet	3.19	0.59	Agree
3.	The confidential records inside the metal filling cabinet are under lock and key	3.19	0.54	Agree
4.	The key of the metal filling cabinet is only within the reach of one authorized person	2.72	0.73	Agree
5.	The key to the door where the confidential records are kept is with one person only	2.22	1.10	Disagree

N=Number of respondent SD=Standard Deviation $\overline{X}$ =Mean

Data from table 1 above shows the responses of admin staff concerning how confidential records are being secured in the College. From the table, one can see that respondents agreed with items 1 to 4 as ways of securing confidential records. However, they disagreed with item 5. This implies that in ASCETA, the key to where confidential records are kept with two or more persons. Table 1 also shows that all the items in the table have standard deviations with lower values. This suggests that respondents are close in their opinions over the items.

Research Question 2
How confidential records are disclosed to unauthorized persons?

Table 2: Means and Standard Deviations of the responses of Admin Staff on how confidential Records are disclosed to unauthorized Persons

N= 32

S/N	Item Statement	$\overline{X}$	SD	Remark
6.	Releasing confidential record to staff without authorization from higher authority	3.06	1.78	Agree
7.	Releasing confidential record to friends without authorization from higher authority	2.81	0.78	Agree
8.	Releasing confidential record to people seeking for specific information without authorization from higher authority	2.97	1.09	Agree
9.	Leaving confidential records within the reach of other office staff	3.06	0.67	Agree
10.	Leaving confidential records within the reach of persons visiting an office(eg. allowing visitor to glance or pip at a mail containing confidential record)	2.91	0.96	Agree
11.	Collecting money from individual(s) and then release confidential records	2.41	0.95	Disagree
12.	Order from above to release confidential record to unsuitable persons	2.34	0.79	Disagree
13.	Release of confidential records by staff as result of threat	2.84	1.08	Agree

N=Number of respondent SD=Standard Deviation $\overline{X}$ =Mean

Table 2 shows that items 6 to 10 and 13 had mean values of more than the cut off point of 2.50. This implies that respondents agree that these items represent how confidential records are disclosed to unauthorized persons. However, respondents disagree with items 11 and 12 as ways of disclosing confidential records to unauthorized persons. Table 2 also shows that all the items have lower values of standard deviations, implying that their opinions are very close concerning the items under consideration.

Research Question 3

How confidential records are removed or altered?

Table 3: Means and Standard Deviations of the responses of Admin Staff on how confidential Records are removed or altered

N= 32

S/N	Item Statement	$\overline{X}$	SD	Remark
14.	Confidential records are removed or altered when they are left within the rich of visitors	3.56	0.72	Agree
15.	Confidential records are removed or altered when they are left within the rich of unauthorized staff members	2.88	0.73	Agree

16.	Confidential records are removed or altered when they are not under lock and key	3.34	0.55	Agree
17.	Confidential records are removed or altered when they are not moved using dispatch book	2.88	0.73	Agree
18.	A confidential records is altered due to the existence of a single copy of that record in the College	2.50	1.08	Agree

N=Number of respondent SD=Standard Deviation $\overline{X}$ =Mean

Data from table 3 shows that all the items had mean values of not less than 2.50. This implies that the respondents agree that the items represent the ways in which confidential records are being removed or altered. Furthermore, the small values of the standard deviations of the items indicated that the opinions of the respondents are very close.

Research Question 4
How can confidential records be more secured?

Table 4: Means and Standard Deviations of the responses of Admin Staff on how confidential Records can be more secured
N= 32

S/N	Item Statement	$\overline{X}$	SD	Remark
19.	Only one officer will have the key to where confidential records are kept	3.47	0.80	Agree
20.	No officer will be allowed to enter into room where confidential records are kept with android mobile phone	3.34	0.70	Agree
21.	No officer should be allowed to post confidential record in any College social media platform	3.41	0.80	Agree
22.	More harsh punishment should be mated to staff found guilty of unauthorized release of confidential record	3.63	0.55	Agree
23.	Periodic capacity building training on confidential Record keeping techniques	3.50	0.57	Agree
24.	Train employees on the importance of confidentiality and data security	3.47	0.57	Agree
25.	Secure physical locations where confidential records are store (e.g. security cameras).	3.47	0.91	Agree

N=Number of respondent SD=Standard Deviation =Mean

Respondents in table 4 agreed that all the items in the table represents how confidential records can be more secured in ASCETA. Furthermore, their opinions are very close going by the smallness of the values of their standard deviations.

VIII. DISCUSSION OF FINDINGS

The findings of this study revealed the following among others that confidential records are kept inside the metal filling cabinet are under lock and key,

confidential record are release to people seeking for specific information without authorization from higher authority, confidential records are removed or altered when they are left within the rich of unauthorized staff members, officers are not allowed to post confidential record in any College social media platform, more harsh punishment are mated to staff found guilty of unauthorized release of confidential records and periodic capacity building training on confidential Record keeping techniques are required. Some of these findings were within the guidelines given by University of Adelaide (2009), Human Resource Management (1999),National Council of Nonprofit Associations (2004) and PIM (2998) respectively.

CONCLUSION

Abia State College of Education (Technical) Arochukwu like any other organization create, handle and keep records for day to day administrative operations. Among such records, some are confidential while others are not. Confidential records need to be protected against disclosure, addition, alteration or removal by unauthorized persons. But in Abia State College of Education (Technical) Arochukwu, some staff are in the habit of disclosing, replacing, adding, removing and mutilating confidential records and information despite some measure in place. In other to reduce the instances of such undesirable behaviour, the researchers set out to find out some strategies that will improve the handling of confidential records. A 25-item questionnaire was designed, constructed and validated. The questionnaire was administered to 32 admin staff. The data collected were then analysed. The result of the analysis revealed the strategies for improving the handling of confidential records in Abia State College of education (Technical) Arochukwu. With these findings in place, the problems of disclosing, replacing, adding, removing or mutilating of confidential records in ASCETA will drastically reduced.

RECOMMENDATIONS

The following recommendations were made based on the finding of the study.
1. Confidential records should not be release to friends without authorization from higher authority.
2. Confidential records should not be left within the reach of persons visiting an office (eg. allowing visitor to glance or pip at a mail containing confidential record).
3. Confidential records should always be under lock and key.
4. There should always be photocopies of confidential records to avoid absence as a result of mutilation or removal.
5. No officer should be allowed to post confidential record in any College social media platform.
6. More harsh punishment should be mated to staff found guilty of unauthorized release of confidential record(s).
7. There should be periodic capacity building training on confidential record keeping techniques
8. Physical locations where confidential records are store most be highly secured.

ACKNOWLEDGMENTS

REFERENCES

[1] Human Resource Management (1999). Personnel Record Keeping & Retention. Policy and Procedure Manual. Retrieved on 15th August, 2020.

[2] Indiana University (2012). Management of Human Resource Records: Personnel Records for Staff and Temporary Employees and Benefit Program Records for All Employees, Retirees, and COBRA Participants. Retrieved on 5th August,2020.

[3] National Council of Nonprofit Associations (2004). Sample Employee Handbook. Retrieved on 5th August,2020

[4] National Pork Board (2010). Personnel Records Management Guide. Retrieved on 5th August,2020.

[5] University of Adelaide (2009). Record Management Handbook. Retrieved on 5th August, 2020.

[6] University of Colorado (2018). University of Colorado Boulder Records Retention Schedule. Retrieved on 5th August, 2020.

[7] United Republic of Tanzania (2013). President's Office Public Service Management. Guidelines and Procedures for Management Personnel Records in the Public Service. Retrieved on 15th August,2020.

[8] West Virginia (2013). Supervisor's Guide to Human Resources Record Keeping Requirements. Retrieved on 5th August,2020.