

# Ethics in Research

## #Research Ethics:

- includes the responsibility of researchers
- to be honest and respectful
- to all individuals who are affected by their
  - ⇒ 1) research studies
  - ⇒ 2) reports of studies' result

### Example of unethical research:

1) Breaking and re-breaking of bones (Nazi)

- to see how many times

- bones could be broken

- before healing failed to occur

2) patients injected with live <sup>affected</sup> cancer

cells

Jewish Chronic Disease Hospital, New York

- 1963

3) [400] men left to suffer with syphilis

- bacterial infection  
- occurred by sexual contact

- but penicillin was available
- place: Tuskegee, Alabama
- Time: 1932 - 72

4) Milgram's study: (1963)

- psychological experiment
- no physical harm
- suffered shame/embarrassment

because of inhuman behaviour

## Ethics codes:

### 1) Nuremberg code:

- ethical treatment of human participants in research

- 1<sup>st</sup> code, 1949

- set of 10 guidelines

25 years later

### 2) National Research Act: 1974

### 3) The Belmont Report: 1979

(i) Individuals give consent to participate in research

{ - children/ disabled/ prisoners can't people

give consent.

- they should be protected

(ii) - not harm participants

- minimum risks

- max. benefits

(iii) should be fair in selecting participants

#### 4) APA Guide:

(i) protect participant from harm.  
physical / psychological

(ii) informed consent:

- before agreement
  - participants have complete info about research
  - about their roles

(iii) participants may feel low.

5) Clinical Equipoise - (comparision)

researcher compares treatments if there's

- 2 cases {  
1) Honest uncertainty  
2) " professional disagreement

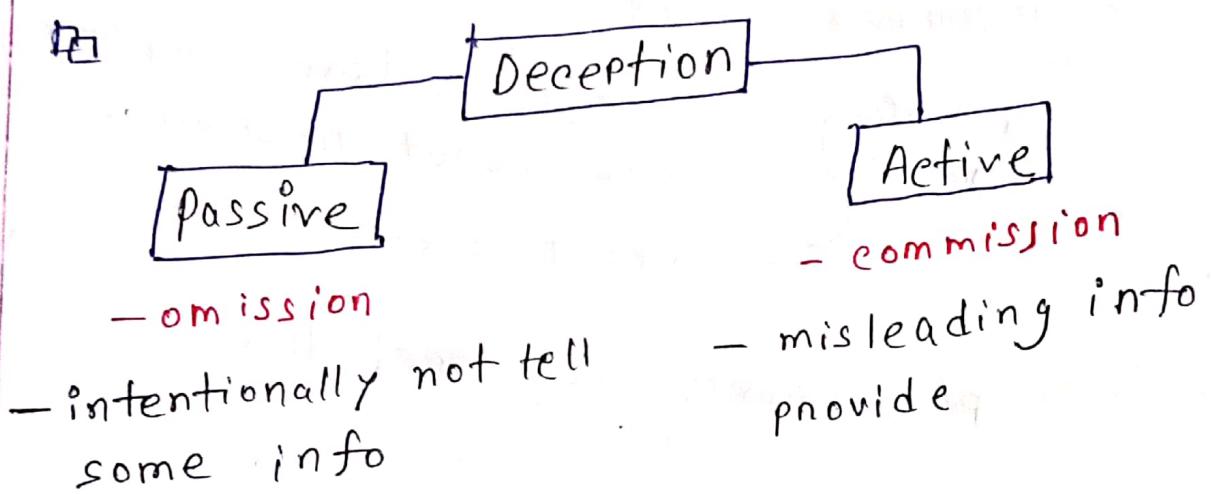
\* Why ensure understanding among participants?

- participants know what will be done

- but don't know why

- simply telling! = complete understanding  
u information

- voluntary participation should be ensured
- => lack of info → they may feel forced to participate.



④ How to justify deception?

- => - significant benefit >> risk
- consider all alternatives to deception
- justify why they're rejected

④ Debriefing (last step) → given to participants  
after completing research

- describes true purpose of study
- use and purpose of deception (later)

## # Confidentiality (acc. to APA guidelines)

- participant's records are kept anonymous

## \* IRB - The Institutional Review Board

- Each institution establish this.
- composed of scientists and non-scientists

## # Reporting of Research:

- no false / deceptive data in reports.
- if significant errors — connection must
- not present other's work as own,
- give credit, if used.

## # Fraud: explicit effort to misrepresent data

↓  
- sort of —

\* Safeguards against fraud: it's a peer review.

- when researcher submits his article, it's needed.

\* Replication: test accuracy by repeating the original / basic procedures.

- repeat prev. research study.

# Plagiarism

Q What is plagiarism?

- the act of stealing someone's work  
attempting to "pass it off" as your own

applicable to : term papers ✓  
photographs ✓  
songs ✓  
ideas ✓

Q Copyright: title 17, U.S. code

✓ - form of protection

- to the authors of

provided to published  
unpublished work

original works

- 1) literary
- 2) dramatic
- 3) musical
- 4) artistic
- 5) intellectual work

provided by:  
U.S Copyright  
Office

- written law
- ↳ Fair Use:
- a **statute** under copyright law
  - allows for the use of **limited** portions of work that has copyright
  - without taking permission from the original author

**purpose:**

- education
- research

↳ limited portion:

"there is **no specific no.** of words, lines or notes that may be taken without permission"

- give credit always
- if unsure, ask for permission

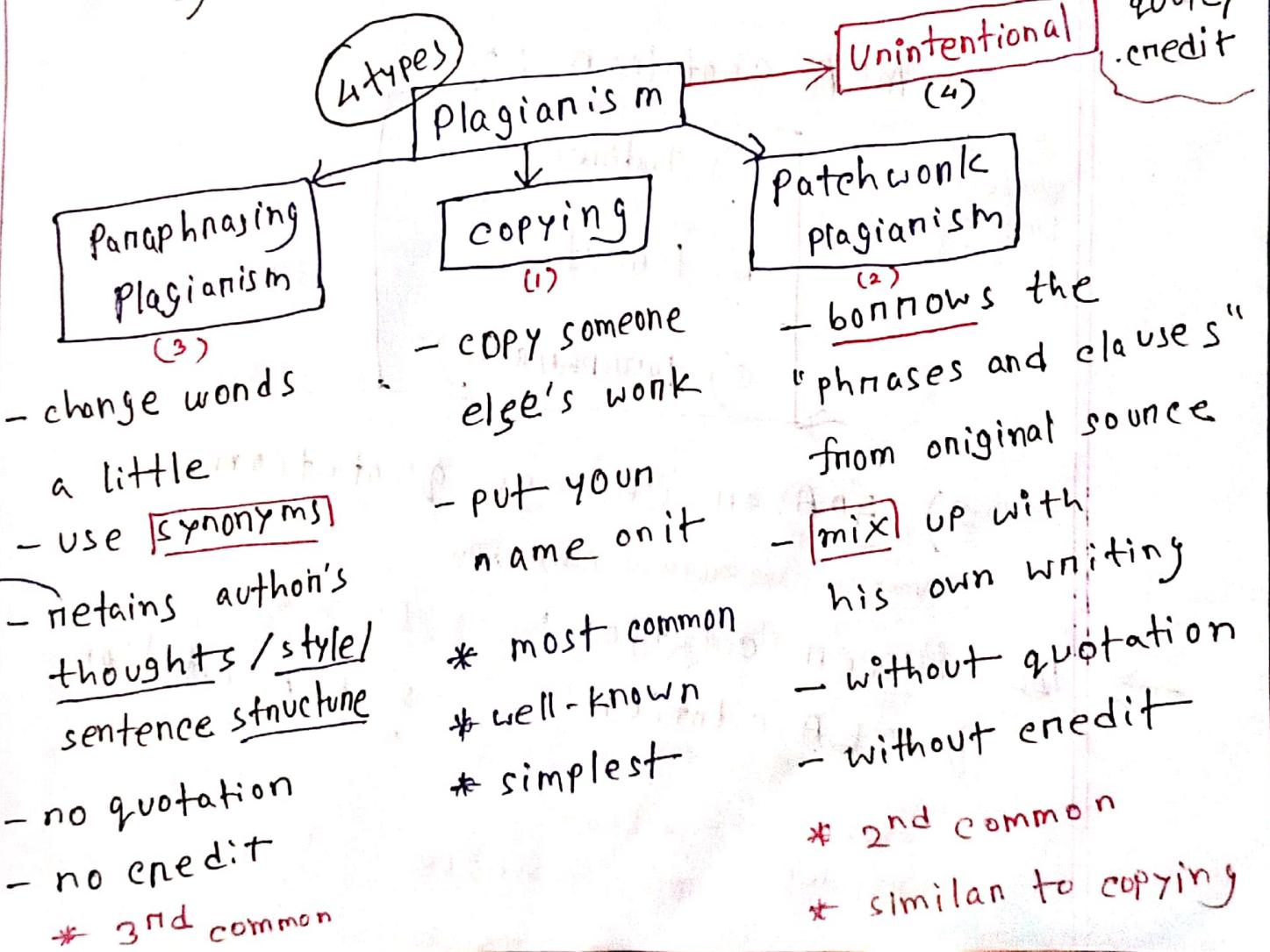
Legal implications: results/consequences  
of being involved in something  
acc. to the law

Ex: SUST's policy:

1) 1<sup>st</sup> offense: fail on assignment

2) 2<sup>nd</sup> " : fail on the whole course

3) 3<sup>rd</sup> " : suspension

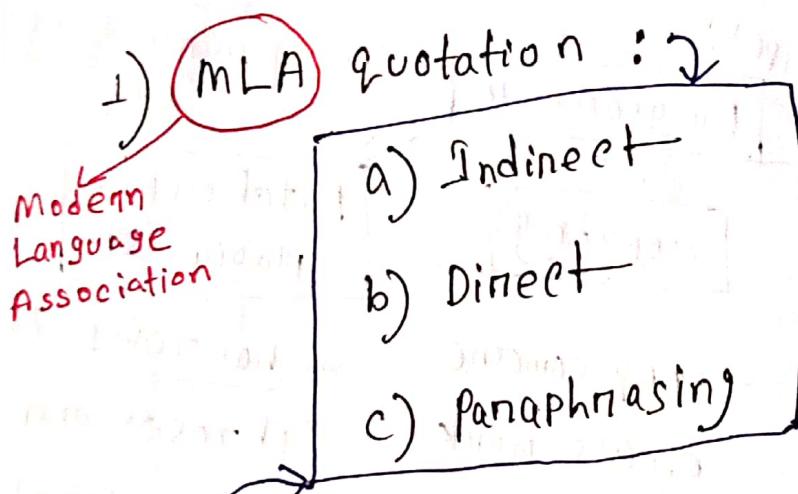


{ quotation - ~~if~~ quote ~~not~~ / credit ~~not~~  
citation - written / source ~~to~~ credit ~~not~~

## \* How to avoid plagiarism?

- Be honest
- give credit of the source
- use your own work as often as possible
- use quotation for other's works

## → # Proper quotation: (2 types)



## → # Proper citation: (type: 2)

- 1) MLA citation
- books
  - articles
- 2) APA citation
- website
  - page (single)

## Cyber Crime

- criminal / illegal activity
- involves unlawful access to computer sys.
- committed on internet
- steals data / information

Ex:- stealing credit card info

- breaking into govt. website

1st cyber crime - finance - 1820

History: person's name: Joseph-Marie

job: textile eng.

invented looms that  
can store design

1st spam email: 1978

1st virus: installed on Apple computer

1982

## category of cyber crime

Target

- use computers to attacks other comp.

Eg. Hacking,  
virus attacks

weapon

- use computers to commit real world crime

Eg. cyber terrorism  
credit card fraud

## Types of cyber crime

1) Hacking

2) Credit Card Fraud

3) Cyber terrorism

4) Computer vandalism (damage)

5) Software Piracy - unauthorized use of another's work

6) Spoofing - send fake mail, ask to provide sensitive data find personal / financial details

**Hacking:** Hacking is a source of threat to security in computer.

- unauthorized access to computer system by a hacker

- Types of Hackers:**
- (3) 1) White Hat Hackers
  - 2) Black "
  - 3) Grey "

**Credit Card Fraud:**

- for personal reasons, an individual uses another individual's credit card
- the owner of the card and the card issuer are unaware of the fact

**Occurrence time:** - online banking  
- shopping

## Solution / Avoidance : (2)

1) One can't use the others credit card

Because of : a) Mobile security code

b) 2-step verification

2) Ethical conduct

- enforced by banks

## ■ Cyber Tensionism:

- use of internet based

attacks

- in tensionist activities

## Prevention:

Ex 1) 7 Iranians working for Iran govt.

Reason: Hacking

Ex 2) Many persons - sent to jail  
- Rawalpindi

Reason: blackmailing on the  
social media

## ■ Computer vandalism:

- damage / destroy data
- transmitting virus

) rather than  
stealing

Prevention: not giving permission to S/W  
without reading the agreements.

## ■ S/W piracy:

- theft of S/W
- through illegal copying of genuine programs.

Reasons: not use original S/W

- costly

Prevention: serious attempt

against the people involved  
in the distribution of pirated S/W

→ taken by some org.

Spoofing: tricking / deceiving  
— computer systems on  
— other computer users

done by: hiding / faking identity

- 3 ways:
- 1) Email spoofing
  - 2) IP spoofing
  - 3) fake identity

Solution:

- 1) keep computer system updated
- 2) use a good antivirus s/w
- 3) Don't open the mail if the sender is unknown.
- 4) ignore mails that has
  - no sender names
  - your name in sender details

## Virus Dissemination:

Virus:

Virus is a malicious s/w

that attaches itself to another s/w.

Solution:

1) keep a regular backup of imp. files.

2) Be careful about opening  
email attachments.

3) Be aware of attachment that

has .exe .vbs .scr .vbe.com .bat .shs .cpl  
.dll .ocx .pif .drv .lnk .bin .sys .eml .nws

above file extensions.

Cyber Laws in  
Pakistan

Electronic Transaction  
Ordinance 2002

- 1st IT Law, ~~introd by govt~~ now
- protects Pak e-commerce
- protect's Pak's critical infrastructure
- taken from foreign law

Electronic / Cyber  
Crime Bill 2007

- promoted by the president of Pak
- ~~introd by govt~~
- 31 dec 2007

- cyber terrorism
- data damage
- electronic fraud
- spoofing
- unauthorized access to code

more about 2007 Law: the crime is a

- people will receive punishment globally  
on locally

- punishment: imprisonment

fine

- **FIA** + investigate and change case

Federal Investigation Agency

#### ■ Safety tips:

- 1) use antivirus s/w.
- 2) Insert firewalls.
- 3) Uninstall unnecessary s/w
- 4) Maintain backUP.
- 5) Check security settings.
- 6) Never give info to strangers
- 7) Learn more about internet privacy.

Cyber security: - branch of computer security  
- related to internet

Objective: establish rules to defend  
to use against attack  
over the internet.

Advantages: - save from critical attacks  
- safe browsing  
- secure incoming / outgoing  
data process.