CYBER SECURITY AND DATA PROTECTION.
TEACHABLE NOTES

Ministry of Education
REPUBLIC OF GHANA

Ghana Education Service (GES)

KATON
360-Degree Knowledge Hub


01
SESSION
Introduction to Data Protection
02
SESSION
Understanding the Data Protection Act, 2012 (Act 843
03
SESSION
Safe Online Practices
04
SESSION
Protecting Teachers' Own Data
05
SESSION
Protecting Students' Data
06
SESSION
Responding to Data Breaches
07
SESSION
Q&A
08
OPTION
REFERENCE

What is Data?

Data refers to facts, figures, or information in any form that can be collected, stored, processed, and shared.
In schools, data often means information about students, staff, and school activities that is written down, saved on a computer, or stored in files.

Examples of Data in Education

Type	Examples
Personal Data	Student name, age, home address, ID number, photograph
Academic Data	Test scores, report sheets, attendance records
Health Data	Medical notes, allergies, disability information
Family Data	Parent names, contact numbers, occupation
Administrative Data	Teacher records, staff schedules, payroll data

In Simple Terms

Data = Information.
It is anything that tells us something about a person, place, or activity.

Two Main Categories of Data

1. Personal Data:
   Any information that can identify an individual e.g., a student's name or ID number.
2. Sensitive Data:
   Information that, if shared wrongly, could cause harm or embarrassment – e.g., health records, exam marks, or disciplinary notes.

Why Data Matters in Schools

- It helps teachers plan lessons, track progress, and support learners.
- It helps school leaders make informed decisions.
- It allows parents to monitor their children's performance.

What is Data Protection?

Data protection refers to the practices, laws, and policies put in place to ensure that personal information is collected, stored, processed, and shared responsibly and securely.
In simple terms, data protection means keeping people's private information safe ensuring it is not lost, stolen, misused, or exposed without permission.

Examples in a school context:

- Keeping student report files locked in a cabinet or password-protected folder.
- Ensuring attendance registers and health records are not left open on desks.
- Avoiding sharing student marks or details on public platforms.

Key Principle:

"Data protection is about respecting privacy and maintaining trust."

Why is Data Protection Important in Education?

To Protects Students' Privacy:
Students' information like health status, academic results, or family background is private. Protecting it helps preserve their dignity and self-esteem.

To Builds Trust:
Parents and guardians trust teachers and schools with their children's data. Maintaining confidentiality strengthens this trust.

To Prevents Misuse of Information:
Personal data can be used for bullying, discrimination, or fraud if mishandled.

For Legal Obligation:
Ghana's Data Protection Act, 2012 (Act 843) requires every institution that handles personal data to ensure it is stored and used lawfully and confidentially.

To Encourage Professionalism:
Responsible data handling demonstrates ethical teaching practices and digital literacy in a modern classroom.

Common Data Risks in Schools

Teachers and schools handle many forms of personal data daily. Below are common risks that can lead to breaches:

Risk Type	Description	Example in Schools
Accidental Disclosure	Sharing data without realizing it's sensitive	Posting student marks in a WhatsApp group
Unauthorized Access	Someone views or uses data without permission	A non-staff member accessing student records
Data Loss	Important files or records get deleted or misplaced	Losing a flash drive with student information
Cyber Threats	Hackers or viruses stealing data	Phishing emails or infected school computers
Weak Passwords	Using easy-to-guess passwords	Passwords like “12345” or “teacher2025”
Physical Insecurity	Leaving documents or laptops unattended	Student files left open on the teacher's desk

Case Study: The Leaked Report Sheet

Scenario:
At a Basic School in Accra, a teacher shared the term's examination results on a WhatsApp group meant for parents. Unfortunately, the message included students' ID numbers and health remarks. Some parents complained that their children's privacy was violated.

Discussion Questions and Answers

1. What kind of data was exposed?
   - Personal data (student names, ID numbers, health information, and academic results).
   - Sensitive data (health remarks).
2. Who was responsible for protecting this data?
   - The teacher who shared the information and the school administration, which oversees data handling procedures.
3. What could the teacher have done differently?
   - Shared only the necessary results privately (e.g., by printing individual reports or using secure online portals).
   - Removed ID numbers and health details before sharing.
   - Sought approval from the headteacher before posting any information online.
4. What are the possible consequences for the teacher and the school?
   - Loss of trust from parents.
   - Complaints to the Data Protection Commission under Act 843.
   - Disciplinary action against the teacher.
   - Reputational damage to the school.

Reflection Questions

1. **What personal data do you handle daily as a teacher?**
   Attendance sheets, student marks, addresses, phone numbers, photographs, health or disciplinary records.

2. **How do you ensure that student data remains secure in your classroom?**
   By locking records in drawers, using strong passwords, logging out of devices, and avoiding public sharing of data.

3. **In what ways does protecting data reflect good teaching ethics?**
   It shows respect for students, upholds integrity, maintains trust, and models responsible digital behavior for learners.

Key Takeaways

- Data protection safeguards trust and ensures ethical teaching.
- Every teacher is a data handler and must act responsibly.
- Ghana's Data Protection Act, 2012 (Act 843) mandates confidentiality and proper handling of all personal information.
- Protecting data is integral to professionalism and digital literacy in 21st-century teaching.

Session 2: Understanding the Data Protection Act, 2012 (Act 843)

The Data Protection Act, 2012 (Act 843) was enacted by the Government of Ghana to ensure that individuals' personal information is handled with respect, care, and responsibility.

Main Purposes:

To protect privacy: Safeguard the personal data of individuals from misuse or exposure.

To regulate data management: Ensure that data is collected, stored, used, and shared lawfully.

To promote fairness and transparency: Require organizations to be honest and clear about how they use data.

To establish accountability: Make institutions responsible for how they handle personal information.

To empower the Data Protection Commission (DPC): Enable the DPC to enforce compliance and apply sanctions when violations occur.

In schools:
The Act ensures that teachers, administrators, and ICT staff handle learners' personal data ethically, securely, and professionally.

Key Principles of Data Protection

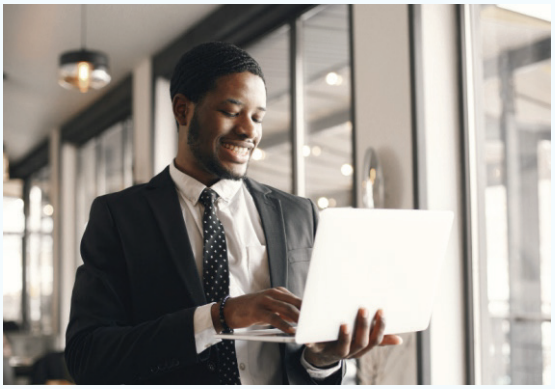
The Act is guided by eight principles that every teacher and school must follow:

Principle	**Meaning in Educational Context**
Accountability	The school or teacher must take responsibility for how data is collected, stored, and used.
Lawfulness and Fairness	Data must be obtained for a legitimate educational purpose (e.g., exams, attendance).
Purpose Limitation	Use the data only for the reason it was collected (e.g., do not use exam data for public comparison).
Data Minimization	Collect only what is necessary for school operations.
Accuracy	Keep data updated and correct (e.g., correct contact numbers or grades).
Storage Limitation	Do not keep data longer than necessary (e.g., old records should be archived securely or destroyed).
Integrity and Confidentiality	Protect data from loss, damage, or unauthorized access (both physical and digital).
Transparency	Inform students and parents how their data will be used and who can access it.

Key Definitions under the Act

Data Controller:
The person or organization that determines how and why data is processed.
Example: A headteacher or school that decides to collect student records or register learners in a database.

Data Processor:
The person who processes data on behalf of the controller.
Example: An ICT officer, administrative assistant, or teacher entering student details into a system.



Data Subject:
The individual whose data is being collected or processed.
Example: A student, teacher, or parent whose personal information is stored or used by the school.

Rights of Data Subjects

Every individual in Ghana has the following rights under Act 843:

Right to Access:
To see what personal data an institution holds about them.

Right to Rectification:
To request correction of inaccurate or incomplete information.

Right to Erasure ("Right to be Forgotten"):
To request deletion of data that is no longer needed.

Right to Object:
To oppose or stop data processing that causes harm or distress.

Right to Complain:
To report a violation to the Data Protection Commission (DPC).

Example:
If a school posts a child's photograph online without permission, a parent can request removal and file a complaint with the DPC.

Case Study: Data Protection Violation in a Ghanaian School

Scenario:

At a school in Accra the ICT department uploaded student's continuous assessment results on the school's public website without restricting access

A student discovered that anyone could view other students' academic and disciplinary records. The issue was reported to the Data Protection Commission (DPC).

Discussion Questions and Answers

1. What went wrong in this case?
   - The school failed to restrict access to sensitive student data.
   - There was a breach of confidentiality and integrity principles.
   - Student data was publicly exposed without consent.

2. Which rights of the students were violated?
   - Right to privacy and confidentiality.
   - Right to object to unauthorized sharing.
   - Right to complain to the DPC.

3. What are the possible legal and institutional consequences?
   - The Data Protection Commission may issue sanctions or fines to the school.
   - The school may face loss of reputation and parental trust.
   - The ICT officer and headteacher may face disciplinary action for non-compliance.

4. How can the school correct its procedures?
   - Restrict access to online data with passwords and permissions.
   - Obtain parental consent before publishing student information.
   - Train staff on Act 843 and safe data management.
   - Register the school with the Data Protection Commission.
   - Develop a data protection policy for the institution.

Reflection Questions and Model Answers

1. What types of personal data are collected in your school?
   - Student names, dates of birth, home addresses, academic records, health details, parents' contacts, and staff information.

2. Who should be responsible for data protection compliance in a school?
   - The headteacher (as data controller) has the main responsibility.
   - Support staff like ICT officers, administrators, and teachers (as data processors) must also comply.

3. How can you promote awareness of Act 843 among your colleagues?
   - Organize staff training sessions on data protection.
   - Display reminder posters on responsible data handling.
   - Encourage secure data practices (passwords, consent forms).
   - Include data protection topics in school meetings and ICT workshops.

Key Takeaways

- The Data Protection Act, 2012 (Act 843) governs all data activities in Ghana.
- Schools are legally required to comply with its provisions.
- Teachers are data handlers and must ensure confidentiality, fairness, and lawful data use.
- Awareness and consistent practice are key to avoiding legal and ethical violations.

Session 3: Safe Online Practices
Understanding Online Safety

What is Online Safety?

Online safety means taking steps to protect yourself, your data, and your digital devices from threats that come through the internet.
In schools, it involves ensuring that both teachers and students use the internet, emails, and digital tools responsibly and securely.

In simple terms:

Online safety is about being smart, careful, and responsible whenever you connect to the internet.

In education:

Teachers practice online safety when they:

- Use password-protected systems to record marks or attendance.
- Avoid sharing student information through unsecured channels.
- Guide students on safe use of social media and online research tools.

What is Cybersecurity?

Cybersecurity refers to the technological and procedural measures used to protect computers, networks, and data from unauthorized access, attacks, or damage.

It is the technical side of online safety focusing on protecting the systems and tools teachers use every day.

Examples of cybersecurity in schools:

- Installing antivirus software on school computers.
- Using firewalls to block harmful websites.
- Enforcing strong password policies for all staff accounts.
- Ensuring data encryption when sharing school records.

Principles of Safe Online Behavior

These are the basic habits and guidelines every teacher should follow to stay safe online:

Principle	Meaning / Application
Verify before you click	Always check the sender and verify links or attachments before opening.
Use strong passwords	Create passwords using a mix of uppercase, lowercase, numbers, and symbols (e.g., ICT@2025safe).
Log out after use	Especially on shared computers in the staffroom or ICT lab.
Update software regularly	Keeps devices secure by fixing weaknesses hackers may exploit.
Back up data	Store copies of lesson plans, marks, and records on secure cloud or external drives.
Use secure networks	Avoid public Wi-Fi for accessing school databases or sensitive emails.
Be mindful on social media	Avoid posting student data, exam materials, or internal school issues online.

What is Cyber Hygiene?

Cyber hygiene refers to daily routines and best practices that keep your digital life clean, organized, and safe – just like personal hygiene keeps your body healthy.

Examples of good cyber hygiene for teachers:

- Installing and updating antivirus software.
- Locking devices when leaving them unattended.
- Avoiding the use of personal laptops for storing student information.
- Enabling two-factor authentication (2FA) on emails and online platforms.
- Deleting outdated files that contain personal or student data.

In essence:
Cyber hygiene is about forming safe digital habits every day.

What is Digital Footprint Awareness?

A digital footprint is the trail of data you leave whenever you use the internet – through emails, posts, searches, uploads, and logins.

Digital Footprint Awareness means understanding that:

- Everything you post, like, or share can be traced and may remain online permanently.
- Teachers should model responsible online behavior to students.
- Your digital reputation should always reflect professionalism, respect, and integrity.

Example:
A teacher who posts inappropriate content on social media risks damaging both their personal reputation and their school's image.

Case Study: Phishing Email at a College of Education

Scenario:

At a College of Education in Ghana, an email was sent to staff claiming to be from the ICT Directorate, asking lecturers to verify their accounts by clicking a link. Several teachers entered their usernames and passwords, which led to unauthorized access to students' records and institutional email accounts.

Discussion Questions and Answers

1. What type of cyber threat occurred?
   - This was a Phishing Attack; a fraudulent email tricking users into revealing login credentials.

2. How could teachers have detected the phishing email?
   - By checking the sender's address (which might not match the official ICT Directorate).
   - Looking for spelling or grammar errors in the message.
   - Noticing the urgent tone ("verify immediately or lose access").
   - Hovering over the link before clicking ;it would show a suspicious web address.
   - What were the possible consequences of this breach?
   - Unauthorized access to confidential student data and staff emails.
   - Data manipulation or loss.
   - Reputational damage to the college.
   - Possible disciplinary action for negligence.
   - Loss of trust among students and staff.

4. What preventive measures should the college implement?
   - Conduct cybersecurity awareness training for all staff.
   - Use official institutional email accounts only.
   - Implement two-factor authentication for all logins.
   - Use spam filters and email verification systems.
   - Establish clear data breach reporting procedures.

Reflection Questions and Model Answers

1. What online tools do you frequently use for teaching, and how do you secure them?
   - Tools: Google Classroom, Microsoft Teams, Zoom, WhatsApp groups, Email.
   - Security: Use strong passwords, enable 2FA, avoid sharing links publicly, log out after use, and update apps regularly.

2. How do you protect your devices and digital accounts?
   - By using antivirus software, locking screens when not in use, backing up data, and not saving passwords on public computers.
3. How can you help students adopt safe online practices?
   - Teach them about cyberbullying and online etiquette.
   - Remind them to think before sharing personal details.
   - Encourage responsible use of school computers and mobile devices.
   - Integrate digital citizenship topics into ICT lessons.

Key Takeaways

- Online safety protects teachers, students, and schools from digital risks.
- Cybersecurity ensures networks and systems remain safe from hackers and viruses.
- Teachers should follow safe online behavior principles and practice good cyber hygiene daily.
- A positive digital footprint builds professional credibility and sets a good example for students.
- Creating a culture of awareness prevents data breaches and promotes trust in digital learning environments.

Session 4: Protecting Teachers' Own Data
Key Concepts and Discussion Points

Understanding Teachers' Data

Teachers produce, collect, and share a wide range of data daily both professionally and personally.

Type	Definition	Examples
Professional Data	Information related to a teacher's employment and work performance.	Staff ID, work email, performance reports, biometric data, posting letters.
Financial Data	Information concerning income, payments, and benefits.	Bank account details, salary slips, SSNIT number, e-payslip credentials.
Health and Personal Data	Private details about health, family, or identity.	Medical records, family contacts, next-of-kin details, vaccination info.
Digital Presence	A teacher's identity and activities online.	Social media profiles, Google Classroom usage, email communication, LMS activity logs.

Risks to Teachers' Data

Risk Type	Description	Example
Phishing & Scams	Deceptive messages used to steal sensitive information.	Fake “salary update” emails requesting login details.
Identity Theft	Criminals pretending to be someone else using stolen data.	Using a teacher's staff ID to create fake accounts.
Data Breach	Unauthorized access to personal or institutional systems.	Weak passwords on GES or HR portals.
Social Engineering	Manipulating someone into giving out confidential data.	A caller posing as “ICT support” to collect login details.
Oversharing Online	Posting private or sensitive info publicly.	Sharing pay slips or staff ID cards on social media.

Strategies for Protecting Teachers' Data

1. Use Strong Authentication:
   Enable two-factor authentication (2FA) for email, HR systems, and LMS platforms.
   Example: Receiving a code via SMS before accessing your account.

2. Separate Work and Personal Accounts:
   Use different emails for school duties and personal matters to reduce risks.

3. Encrypt Sensitive Files:
   Use password-protected documents or encryption tools to secure staff and student information.

4. Manage Digital Footprints:
   Regularly review privacy settings, remove old posts, and ensure your online image reflects professionalism.

5. Secure Physical Devices:
   Lock laptops, phones, and flash drives. Never leave them unattended in public places.

6. Be Cautious with Public Wi-Fi:
   Avoid logging into official systems using café or hotspot networks.

7. Limit Sharing:
   Only share data with authorized individuals and through official channels.

Ethical and Legal Dimensions

- Teachers are data handlers, meaning they manage information that must remain confidential.
- Under Ghana's Data Protection Act, 2012 (Act 843), sharing staff or student data without consent is a violation.
- Schools and GES must train staff and enforce data protection policies.

Activity: Social Media Safety Audit

Participants review their social media accounts and make one privacy adjustment (e.g., hide phone number, make profile private).
Then, discuss:

“How can your social media posts affect your professional reputation?”

Definitions of Key Terms
Terms and Explanation

Professional Data is Work-related information like staff ID, work email, or performance evaluations.
Financial Data is Any information about a person's financial identity or transactions.
Health and Personal Datais Information about a person's medical, family, or personal life.
Digital Presence is Your identity and behavior online emails, posts, and digital interactions.
Authentication is The process of verifying a user's identity before allowing access (e.g., password + code).
Personal Accounts is Private digital profiles (emails, social media) used for individual communication.
Encrypt is Converting data into a secure, unreadable format unless unlocked with a password.
Manage Digital Footprints is Monitoring and controlling what appears about you online.
Physical Devices is Tangible hardware like laptops, phones, and flash drives.
Wi-Fi stands for Wireless Fidelity which is A wireless network connection to the internet.
Ethical and Legal Dimensions is The moral and lawful responsibilities guiding how teachers use and share data.
Data Handlers are People (like teachers) who collect, use, or store personal data of others.
Data Mapping is The process of identifying where and how data is stored and transferred within a system.
Google Drive is a secure cloud storage service used to save, share, and access files online.
Identity Theft is When someone steals your personal data to impersonate you or commit fraud.

Case Study: The Fake HR Portal

Scenario:
In 2023, a fake "GES HR Update Portal" circulated on WhatsApp, asking teachers to log in with their staff IDs and passwords. Hundreds of teachers entered their details, exposing sensitive employment and financial information. Some noticed fraudulent deductions afterward.

Discussion Questions and Suggested Answers

1. What data protection mistakes did the teachers make?
- They failed to verify the authenticity of the HR link.
- They entered sensitive login details on an unverified platform.
- They shared personal credentials without confirming from official GES channels.

2. How could this incident have been avoided?
- By verifying with GES before clicking suspicious links.
- Using official portals only (e.g., HRMIS website).
- Being trained on phishing and cybersecurity awareness.

3. What immediate steps should affected teachers take?
- Change passwords immediately.
- Report the incident to the school's ICT coordinator or GES.
- Monitor bank and payroll accounts for unusual activity.
- Activate two-factor authentication on accounts.

4. What role should the school or GES play in such incidents?
- Investigate and alert all staff about the scam.
- Provide cybersecurity awareness sessions.
- Implement official communication channels and secure HR systems.

Reflection Questions and Answers

1. How do you secure your personal and work data?
- By using strong passwords, enabling two-factor authentication, encrypting documents, and backing up data securely.

2. What online habits expose you to risks?
- Clicking unverified links, reusing passwords, oversharing on social media, or using public Wi-Fi for work logins.

3. How can teachers support each other in protecting professional data?
- By sharing safety tips, reporting suspicious messages early, and promoting a culture of caution and accountability within the staff group.

Key Takeaways

- Every teacher handles personal and professional data daily.
- Protecting one's own data is as important as protecting students' data.
- Ethical and responsible data handling builds trust and professionalism.
- The Data Protection Act (2012, Act 843) applies to both personal and institutional data.
- Digital awareness and strong cybersecurity habits are essential for 21st-century educators.

Session 5: Protecting Students' Data
Key Concept Explanations

1. Privacy and Confidentiality

- Privacy is a student's right to decide who can access their personal information.
  Example: A student's health condition should not be discussed publicly without consent.
- Confidentiality is the teacher's duty to protect and not disclose student information to unauthorized persons.
  Example: A teacher should not share student marks on a public platform.

- In simple terms:
- Privacy belongs to the student. Confidentiality is the teacher's responsibility to protect it.

2. Security of Educational Data

This refers to the measures taken to keep all student data safe from loss, damage, or unauthorized access both in physical files and digital systems.
Examples include:

- Locking file cabinets containing student records.
- Using passwords or encryption on computers storing student information.
- Limiting access to only authorized staff (e.g., headteachers, class teachers).

3. Password-Protected Systems

These are digital platforms or files that require a secret password or passcode before access is granted.
Example: A school database or a teacher's Excel sheet protected with a password so only authorized users can open or edit it.
Purpose: Prevents unauthorized persons from viewing or changing sensitive data.

4. Restricted Data
This refers to information that only specific, authorized individuals are allowed to access due to its sensitivity.
Example: Student disciplinary reports or medical information should only be seen by school management or health officers not all staff.

5. Personal Identifiers
These are details that can uniquely identify a specific student or individual.
Examples:

- Full name
- Student ID number
- Address
- Date of birth
- Photograph

Such data must be handled carefully because it can easily be linked to an individual.

6. Data Breach
A data breach occurs when confidential or personal information is accessed, shared, or disclosed without permission.
Example: A teacher leaving a laptop unlocked and another person accessing student grades without consent.
Consequences may include loss of trust, legal action, or disciplinary measures.

Case Study: Mrs. Amponsah's Laptop Incident Questions and Answers

1. What data protection issues are raised in this case study?
- Unauthorized access to students' personal and academic records.
- Breach of confidentiality : student information was shared without consent.
- Lack of data security: laptop left unattended without password protection.

2. How could Mrs. Amponsah have ensured that the spreadsheet was protected from unauthorized access?
- By locking her laptop or using a strong password.
- Encrypting or password-protecting the spreadsheet file.
- Storing the data on a secure, institutional system rather than a personal device.
- Ensuring she logs out or locks the screen before leaving her desk.

3. What are the potential consequences of this breach of confidentiality?
- Loss of trust between students, parents, and teachers.
- Emotional harm to students or families due to exposed personal information.
- Disciplinary or legal action under the Data Protection Act, 2012 (Act 843).
- Damage to the school's reputation.

4. What steps should the school take to prevent similar incidents in the future?
- Provide training for teachers on data protection and cybersecurity.
- Develop and enforce a data protection policy.
- Require password protection and encryption for sensitive files.
- Regularly audit school devices and storage systems for compliance.
- Encourage use of official GES or school email accounts for data exchange.

Lesson Learned

Even if the teacher's intentions are good, sharing student information without proper security or consent violates privacy.
Teachers must always use approved, secure channels for data sharing and model ethical digital practices.

Reflection and Discussion Questions (with Answers)
Questions and Answers

1. How can data protection improve students' confidence in teachers and schools?
- When students know their personal data is safe, they trust teachers more.
- It fosters respect, security, and openness in learning environments.
- Parents and students are more likely to share accurate information when they are confident it will remain confidential.

2. What practices can teachers adopt to maintain the confidentiality of student data?
- Avoid sharing marks or reports on public platforms (e.g., WhatsApp groups).
- Lock files and password-protect devices.
- Discuss student performance only in private or authorized meetings.
- Obtain consent before using student data for displays or publications.

3. How can institutions balance transparency (e.g., sharing results) with privacy rights?
- Share only necessary information with the right audience (e.g., individual report cards instead of public lists).
- Use secure online portals for result checking instead of open groups.
- Inform parents and students why and how their data is used.

4. What role should the Ghana Education Service (GES) play in monitoring data protection compliance?
- Develop and enforce clear data protection policies for schools.
- Train teachers and administrators regularly on Act 843.Conduct compliance checks and audits in schools.
- Collaborate with the Data Protection Commission to handle violations and provide guidance.

Key Takeaways

Data protection in education is not optional it is a legal and ethical duty.
Teachers must respect student privacy and handle records securely.
Confidentiality builds trust, professionalism, and integrity.
Schools and GES share responsibility for enforcing Act 843 compliance.

Session 6: Responding to Data Breaches

1. What is a Data Breach?
A data breach occurs when confidential, personal, or sensitive information is accessed, disclosed, or shared without authorization.
In schools, this could mean exposing students' grades, health data, or contact information to unauthorized individuals ;either accidentally or deliberately.

2. Human Error
Human error refers to mistakes made by people that lead to a data breach.
Examples:
- Sending student records to the wrong email address.
- Uploading files with personal data to public online platforms.
- Forgetting to log out of a shared computer.

3. Weak Security Systems
Weak security systems mean the school's digital or physical security measures are inadequate to protect data.
Examples:
- Using outdated antivirus software.
- No password protection on school databases.
- Storing student records in unlocked cabinets.

4. Cyberattacks
A cyberattack is a deliberate attempt by hackers or malicious actors to access or steal data.
Examples:
- Phishing attacks (fake emails tricking staff into sharing passwords).
- Malware or ransomware infections that lock or steal school data.

5. Negligence
Negligence happens when staff fail to follow proper data protection procedures, leading to data exposure.
Examples:
- Leaving files or laptops unattended.
- Not updating security passwords.
- Ignoring data protection training or school policies.

6. Unauthorized Access
This occurs when someone views, copies, or shares data without permission.
Examples:
·A teacher accessing student counseling reports they are not authorized to view.
·A student hacking into the school's grading system.

Case Study: Data Breach in a Ghanaian School

Scenario Recap:
An ICT teacher uploads a spreadsheet with students' names, results, and contacts to a public Google Drive link. The file goes viral, leading to embarrassment and online bullying.

1. What type of data breach occurred in this case?

This is an accidental data disclosure or unauthorized public sharing of personal and academic information.
It combines human error and weak digital security.

2. What immediate actions should the teacher and school authorities take?
- Remove the file immediately from the public link.
- Notify the Head-teacher and Data Controller of the school.
- Report the incident to the Data Protection Commission (DPC) as required by Act 843.
- Inform affected parents and students about the breach.
- Document what happened and actions taken for accountability.
- Provide counseling support for affected students if necessary.

3. Which stakeholders should be informed?
- Headteacher / School Management.
- Data Protection Commission (DPC).
- Parents and affected students.
- District or Municipal Education Directorate.
- Possibly the Ghana Education Service (GES) if the breach is severe

4. What preventive measures could have avoided the incident?
- Training teachers on safe data handling and Google Drive permissions.
- Using school-approved secure platforms for data storage.
- Encrypting files or using password-protected access.
- Regular audits and monitoring of data-sharing practices.

5. How should the institution rebuild trust with affected students and parents?
- Offer a formal apology and explain corrective actions.
- Demonstrate transparency about what was done to fix the problem.
- Provide training for staff to prevent recurrence.
- Introduce stricter data sharing policies and regular communication with parents on data safety.

Reflection and Discussion Questions (6.6)

1. How can data breach preparedness improve accountability in schools?

Preparedness ensures that everyone knows what to do when a breach occurs, minimizing harm.
It promotes:
- Responsibility among teachers and administrators.
- Documentation and reporting, which make actions traceable.
- Trust and transparency between schools and parents.

2. What systems should institutions implement to ensure quick detection and reporting of data incidents?
- Incident response plan (clear steps for identifying and reporting breaches).
- Centralized digital monitoring system for data access logs.
- Regular training and drills for staff.
- Appointing a Data Protection Officer (DPO) to handle data issues.
- Automatic notifications for suspicious activity in digital systems.

3. How can teacher training contribute to reducing data breach risks?
Training helps teachers to:
- Recognize phishing and cyber threats.
- Follow secure data storage and sharing procedures.
- Understand their legal and ethical duties under Act 843.
- Build a culture of data protection in the school.

4. What ethical responsibilities do teachers have when they become aware of a breach?
Teachers must:
- Report immediately to the Head-teacher or Data Controller.
- Avoid covering up incidents to protect colleagues.
- Respect confidentiality while investigations are ongoing.
- Support affected students, ensuring data is not further exposed.

Summary (Key Takeaways)

Concept	Explanation
Data Breach	Unauthorized access or exposure of personal data.
Human Error	Mistakes by staff that cause breaches.
Weak Security Systems	Lack of proper digital protection.
Cyberattacks	External hacking or phishing attempts.
Negligence	Failure to follow security procedures.
Unauthorized Access	Viewing or sharing data without permission.
Response Steps	Identify → Report → Contain → Notify → Prevent future breaches.

Ministry of Education
REPUBLIC OF GHANA

Ghana Education
Service (GES)

KATON
360-Degree Knowledge Hub