Please refer to the online lesson plan on the DT Hub to access all website links and additional resources.

## Learning hook

Teacher shows the *Powerpoint presentation Futureproofing data: Futureproofing in the past* (slides 1–10 only), using the presentation notes accompanying each slide to supply background that is of interest for each.

* It is not necessary to read the presenter notes verbatim, but rather to extract those parts that will be of interest. (Total 10 min max)

After viewing, discuss the following with students:

* We have seen data stored on rock surfaces, caves, papyrus, scrolls, books, wax and wood. We have seen data that has lasted thousands of years and clearly reveals the past. In some cases the data is still in perfect condition. Which of these media have proven to be the best methods of preservation?

Comment to students:

* It is not as if printed records are necessarily superior to digital ones.
* There are advantages and disadvantages to both. Digital data can certainly be lost without trace; many users of computers have had hard disks fail without ever making a backup.
* But printed books too can easily be destroyed: the largest and most precious library in the ancient world at Alexandria was destroyed by fire and the invaluable handwritten books it contained were lost forever.

## Learning map and outcomes

* Students will critically compare past information recording techniques to digital data techniques
* Students will investigate actions, devices and events that are potential risks to data storage, excluding those of theft
* Students will investigate the impact and opportunities created through obsolescence of data storage devices

## Learning input

**Obsolescence**

Show students the *Powerpoint presentation Futureproofing data: Futureproofing in the past* (slides 11-20), and use the teacher notes accompanying each slide to supply background for each.

* Although presentation notes have been provided on each slide, only give students the date and description of the operation of each storage medium. (Total 10 min max).

If you have access to the actual storage devices and/or media, then display them also.

If enough physical examples exist then have a “Hardware Expo”.  Broaden the experience beyond storage devices by including input, output and processing devices as well. Cut out the numbers provided on the following worksheet to identify each item. Cut out separate strips and issue as many as desired to each student. Students research and complete as much as possible of the worksheet (*Hardware Expo*) provided. If wished, they can then be required to present one item to the class.

If enough physical examples exist then have a 'Hardware expo'. Students research and complete as much as possible of the worksheet *(Hardware Expo)* provided.

Discuss with the class the history of the evolution of data storage over the years, and your personal experience of it.

**Deletion**

Many of us have had experience of accidentally deleting a file. Explain to students that, if the file is important enough to us, it is sometimes possible for it to be retrieved, as deletion on a hard drive does not erase the data immediately, but merely removes the item indexing it. Until it is overwritten, the data is still there. This is often used by law enforcement agencies to retrieve incriminating digital evidence.

**Damage**

Read the following to the class:

'A destructive scam email that infects computers and holds them hostage has successfully targeted at least 10,000 Australians since it was detected this week. The email, purporting to be from energy company AGL, sends a fake bill and prompts the recipient to click on a link to download a copy. It then saves a .zip file on the computer which, when extracted, locks the machine down using malware known as "ransomware". The recipient is prompted to pay $A880 to unlock it. A senior analyst at a global cybersecurity firm said once the file has downloaded ransomware the only way to get rid of it is to restore from a backup or to wipe the computer and start over again.'

Source: '*Thousands targeted by "ransomware" email scam which copies AGL Energy bills*' Georgina Mitchell - accessed June 3 2016

This example of a scam email is known as a Trojan horse (named after the ancient Greek story of the wooden horse that was used to help Greek troops invade the city of Troy). It is a form of malware, where a malicious program, pretending to be something innocent, tricks a user into executing it.

Explain that viruses can corrupt data, delete files altogether, erase a hard disk and send infected files to contacts in your address book. Tell students: Computer viruses can spread when you:

* launch an infected application
* use a disk that contains infected files
* open an infected attachment
* download infected files from the Internet.

Discuss data loss as a result of malware or viruses.

Discuss with the class what precautions can be taken to protect computers against data loss by viruses and malware.

## Learning construction

Show the students the PowerPoint presentation *Futureproofing data: Data storage research* (slide 21).

Students in eight groups research each of the media listed in this slide, and then complete the missing information.

A research summary is provided here for your reference:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Storage medium** | **Year launched** | **Capacity** | **Type of medium** | **Estimated life expectancy** |
| Cassette tapes | 1962 | 400 KB | magnetic | 10–20 years but can wear out with use |
| Floppy disks | 1971 | 1.44 MB | magnetic | 2–15 years |
| Zip disks | 1994 | 100 MB/750 MB | magnetic | 2–10 years but can wear out with use |
| CD-R/DVD-R | 1990/1997 | 700 MB | optical | 5–25 years |
| Hard disk drive | 1960s | 3.75 MB (now 10 TB) | magnetic | 3–5 years |
| USB Flash | 2000 | 8 MB | Solid state | 10 years or 100,000 cycles |
| SSD Solid State Flash drive | 1989 | 250 MB–1 TB | Solid state | Various ratings are given: 10 years or 100,000 cycles or 20 GB writes per day for 3 years |
| Cloud storage | 1960s | ? | Magnetic, hard drives on distributed servers |  |

**Lucky dip research**

Print one copy of the *PDF resource provided: Lucky dip scenarios*.

These 'data dilemmas' should be cut into individual strips and placed in a lucky dip.

These scenarios include retrieving deleted files and data loss as a result of viruses or malware.

Students (pairs are suggested) select one scenario, developing their response to the scenario given.

## Learning demo

Allow 10–15 minutes, after which pairs read their scenario aloud then informally report their response back to the class.

## Learning reflection

Ask students to discuss the following:

* In the first set of slides we saw data that has been successfully preserved for over 30,000 years.
* Do you think this will be true of today's important data 30,000 years from now?
* Will any of these various data storage media be readable at that time?

## Curriculum links

| Links with Digital Technologies Curriculum Area |
| --- |
| **Strand** | **Content Description** |
| **Processes and Production Skills** | Evaluate existing and student solutions against the design criteria, user stories, possible future impact and opportunities for enterprise (AC9TDI10P10). |

## Assessment

Note: Criteria are cumulative

|  | **Quantity of knowledge** | **Quality of understanding** |
| --- | --- | --- |
| **Preserving data** | Little or no evidence of understanding | Student is able to identify up to 5 distinct data storage devices | Student is able to describe in some detail up to 5 distinct data storage devices | Student is able to identify the strengths and weaknesses of a number of data storage devices | Student is able to describe a number of scenarios that present difficulties in data retrieval, and suggest workable solutions to these. |
| **Optional score** | 0 | 1 | 2 | 3 | 4 |