Explain the requirements for language, tone, image, and presentation for different documents

Different documents require different methods and presentation in order to be effective. A few examples are as follows:

Emails: language will be formal and personal, but succinct, in order to convey information as quickly as possible in a professional setting. Tone depends on the audience receiving the email – emails sent to superiors within an organisation will have a formal and professional tone, with no "beating around the bush", whereas an email to a colleague of the same level may be a little more informal and might include something resembling "small talk". The image of an email also depends on the context – an email on behalf of a company would contain imagery, logos, and colour schemes depending on the company's branding, whereas a mass-email attempting to make a sale would contain imagery related to the products being advertised. Presentation is often in a "memo" style, with the sender, recipient(s), subject, then the main body of the message.

Reports: language will be impersonal and formal, with no irrelevant information. The tone would be somewhat matter-of-fact and information would be presented with little mention of opinion, unless required. Image would be text-heavy, with the only imagery being that which is relevant to what is being discussed. Presentation would be a long word document, with as many pages as is required to convey the information.

Posters: posters are usually produced with the intention of drawing attention to something. As such, language will be emphatic and exciting, with dynamic words. Tone would remain professional and informative, but the exciting language would add an informal level that would appeal to the relevant audience. The image of the poster would be eye-catching, with bright colours and large fonts and imagery to draw the attention of passers-by. Presentation would be kept to a single page, but could by any size ranging from A5 upwards.

Explain how to integrate images into documents

Many word-processing and messaging programs have in-built capabilities to embed images within documents. Images can be added from with a computer's files, then formatted to fit within the document, and moved to wherever is desired. For example, in Microsoft Word, one clicks the "Insert" dropdown, clicks (for example) "Pictures", then "From File". One then selects the desired image, clicks "Open", and it is placed in the document, where the cursor is. The image can then be clicked and dragged to wherever is desired within the document. Images can be aligned with text, or attached on the end of documents and referenced with a number, both next to the image and within the text.

Another way to integrate images is to use the "Copy" function of the computer (either right-click > Copy, or Ctrl+C (PC)), then right-click and "paste" (or Ctrl+V (PC)) it into the desired space in the document.

Describe how corporate identity impacts upon document production

Corporate identity impacts production by providing guidelines on the presentation of a document. For example, some companies will have branding that incorporates fonts, colours, and imagery (such as logos), which an employee is restricted to using when producing documents on behalf of the company. This also includes slogans and straplines, which may be required to be incorporated into, for example, a business card, or some other promotional material.

Explain the requirements of data protection, copyright, and intellectual property legislation relating to document production

Personal or sensitive data can't be published publically due to data protection laws– and there are dangers that an employee may leave sensitive documents, or USBs containing sensitive documents, in a public place. This means USBs may be encrypted or password-protected, and document production can be delayed if an employee doesn't have the correct password or authorisation.

Imagery, likenesses, and some literary items are protected by copyright laws. As a result, companies must not copy or use another's intellectual property (works or design), else they face legal action from the copyright owners.

Copyright protection will apply automatically if a company produces original literary, dramatic, musical, or art work. For most companies, this constitutes logos, straplines/slogans, and vision statements. It gives a company the ability to demand a royalty or a license fee if allowing others to reproduce or share the work. This also means a company can be charged fees for using content from other organisations, so companies must be careful not to plagiarise if they are unwilling to literally pay the price.

Describe organisational procedures for version control

A common organisational procedure relates to keeping track of how and when files are edited with, for example, a numbering system for versions (Version 4.0, 4.1, etc.). Whole numbers stand for major changes and edits, whereas decimal numbers are used when changes are minimal and not major enough for a completely new version. As edits can be deliberate, malicious, or accidental, it is important for organisations to keep track of versions, when said versions were edited, and what changes were made. This makes it easier for mistakes to be reversed, and for investigations into why changes were made. In addition, a master copy can be kept in a secure place, such as an encrypted or password-protected USB device, as a back-up in case of loss of data or irreversible edits.

Describe security requirements relating to document production

Strict security requirements are often crucial for protection from consumer laws, and data-protection laws. Sensitive documents, such as consumers' private information or even "trade secrets", must be protected from access by unauthorised persons. There are a number of ways of doing so, including the following:

- Passwords and usernames require an employee to confirm their level of authorisation in order to access documents. By managing an account's privileges and authorisations through a computer network, it is very simple to set a level of authorisation that is enforced by the programming, instead of manually.
- Security software, such as firewalls, anti-spam software and antivirus software (which often also protects against malware and network attacks), can offer a layer of protection against external unauthorised access. Often, a virus or malware can grant a hacker access to sensitive files – but with security software, coupled with secure passwords, the risk of this happening is lowered. It is important to keep the software updated, as new versions will protect against newly-generated threats.

- Some documents, such as Word documents, can also be made “read-only” for security. In this case, the only people who can edit a document are those who are authorised, otherwise the document can only be viewed.
- Physical documents should be stored in a secure room, with security measures that only allow access to authorised personnel. This may be a simple lock-and-key system, or “smart locks” that require key-cards to be scanned or swiped, or require PIN numbers to be entered on a PIN pad.
- Physical documents should also have an electronic backup, again protected with encryption or passwords.