Legal and ethical issues in business communication

Unit 4 –Business Communication

Assignment 3 – Legal and Ethical issues

Task 4

Data Protection Act 1998

Businesses store information about people inside their organisation. The Data Protection Act protects the information held about people from being misused. The information stored must be:

- Obtained fairly and lawfully
- Used only for the purposes stated during collection
- Adequate, relevant and not excessive in relation to the intended use
- Accurate and up to date
- Not kept for longer than necessary
- Processed in line with your rights
- Subject to procedures to prevent unlawful processing, accidental loss, destruction and damage to personal data
- Protected from transfer to an area outside the European Economy Area unless adequate protection exists for that data in the area

This act means that Trinity Communications can’t use anyone’s personal details without consent from the actual person. For example, they can’t give out someone’s address or date of birth unless they have permission from that person. If they do keep information on customers or members, they have to make sure that the information is secure in a protected database so that strangers can’t randomly access it. Trinity Communications has to

ensure that they have a back up of all personal information just in case the original data gets corrupted or deleted. If Trinity Communications don’t adhere to the Data Protection Act, they could face nine fines totaling £1, 120, 000.

Computer Misuse Act

This is a law in the UK that legislates against certain activities using computers, such as hacking into other people’s systems, misusing software or helping a person to gain access to protected files on someone else’s computer. The Computer Misuse Act is split into three sections:

- Unauthorised access to computer material
- Unauthorised access to computer systems with intent to commit another offence
- Unauthorised modification of computer material

This act means that Trinity Communications can’t use illegal pirates of software or any form of program. They’re not allowed to access other people’s computer data without permission. They’re not allowed to use unauthorised data as a form of blackmail. It is illegal for Trinity Communications to gain access to a computers data with the intention of altering or deleting it. In addition Trinity Communications cannot plant viruses. If Trinity Communications fail to adhere to this Act, they could face two types of penalties, summary and indictment. Summary penalty can land trinity Communications into prison for 12 months or a fine of up to the statutory maximum. Indictment penalty can land Trinity Communications into prison for 2 years and/or a fine.

Freedom of Information Act

This Act provides individuals and organisations with the right to request information held by a public authority. The public authority must tell the applicant whether it holds the information, which it must supply within 20 working days. There are some exemptions to this Act. E. g. If the cost of a request for information exceeds an appropriate limit, the public authority may decide to decline the request because they might opt to serve a greater public interest. If there is a dispute, Commissioner’s Office may investigate and deem whether the information should be released or not.

Trinity Communications must treat all requests for information equally, they must consider any information they release as if it was being released to the world at large. Trinity Communications cannot, fail to respond adequately to a request for information, fail to adopt the model publication scheme, fail to publish the correct information, deliberately destroy, hide or alter requested information to prevent it being released. If Trinity Communications fail to adhere with this Act, they would be committing a criminal offence which could land them in prison.

Copyright Act

Copyright gives the creators of some types of media rights to control how they’re used and distributed. For example, when you buy software, Copyright Act forbids you from: giving a copy to a friend, making a copy and then selling it, using the software on a network (unless the license allows it) and renting the software without permission of the copyright holder.

This Act means that Trinity Communications must have a valid copy of any software they decide to buy. They cannot sell original copies of purchased software to another party; if Trinity Communications fail to do this, fines from £200 – £150, 000 for each work infringed and jail time.

Discrimination Act

The Act simplifies, strengthens and harmonises the current legislation to provide Britain with a new discrimination law which protects individuals from unfair treatment and promotes a fair and more equal society.

The nine main pieces of legislation that have merged are:

1. The Equal Pay Act 1970
2. The Sex Discrimination Act 1975
3. The Race Relations Act 1976
4. The Disability Discrimination Act 1995
5. The Employment Equality (Religion or Belief) Regulations 2003
6. The Employment Equality (Sexual Orientation) Regulations 2003
7. The Employment Equality (Age) Regulations 2006
8. The Equality Act 2006, Part 2
9. The Equality Act (Sexual Orientation) Regulations 2007

This Act means that Trinity Communications cannot discriminate to anyone in any form or way; this can range from pictures to words and even verbal abuse. They’re not allowed to harass and victimise anyone in the basis of age, disability, gender, race, religion or belief. They must treat everyone

equally regardless. If Trinity Communications fail to suffice to this law, they could face time in prison and heavy fine.

Business Ethics

These are moral principles concerning acceptable and unacceptable behaviour by businesses. There are codes of practice in an organisation to maintain business ethics on: the use of emails, internet, whistle-blowing, organisational policies and information ownership. Trinity Communications can’t use email to send large documents/attachments, especially to large numbers of people; this will stop information/personal data from being leaked into the wrong hands. Trinity Communications shouldn’t use emails as a substitute for face-face/telephone communication with colleagues because it is important to maintain a good interpersonal relationship with colleagues.

In regards to the internet, there are many codes of practice what Trinity Communications can and cannot use the internet for. There are lots of codes of practice in regards to selling on the internet that Trinity Communications has to follow.

Whistle-blowing is an employee who raises concern about a business’s practice, either inside or outside the organisation. The concern may relate to fraud, crime, danger, or any other serious risk that could impact on customers, colleagues, shareholders, the public, the environment or the organisations reputation. Whistle-blowers may receive legal protection through the Public Interest Disclosure Act.

Organisations may have many policies to ensure that their businesses practices with regard to information can be done more ethically. This could be anything from how they manage information to ensuring marketing and other business practices are fair and just.

Information Ownership is simple – if you create information in your day-to-day work, then you should be responsible for it. E. g. writing a report following a member of staff's annual review. This report is confidential to some degree and should only be viewed by a select group of people. Trinity Communications can't show this information to anyone outside the selected group. As the information owner, Trinity Communications would be responsible for protecting this document to an appropriate degree.

Organisations have to store and manage countless pieces of information, some being far more important than others. At the heart of any information systems are two fundamental issues ensuring that: the organisation receives the information it requires and the appropriate member(s) of staff receive the information.

To make sure that information is managed appropriately, a number of procedures and policies have to be put in place, concerning: security of information, backups, health and safety, organisational policies and business continuance plans.

Security Information

Much information security management focuses upon digital data; however, the subject also covers records and knowledge management. It is important

for businesses like Trinity Communications to have the right information available as and when they need it, in order to make good business decisions. For this reason, many companies keep their information on IT systems, but as reliance on technology increases, so does the risk posed by system failure and malicious attacks e. g. viruses. The IT security policy should take into account the common risks to the information that their business relies upon. This policy might include secure login identification for using IT systems and controls that limit access to information.

Backups

Large businesses have developed business continuity programmes to try and minimise the risk of losing vital business information stored on IT servers. For Trinity Communications this should involve producing backups of information stored on the servers – some companies will create a backup every hour, while others will do this less frequently. This means that if live information is destroyed or damaged, a copy of this will be available on the backup services enabling a company to continue with as little disruption as possible. Backups are normally stored on separate hardware from the live versions of the information to ensure they’re protected. This means that if the live version corrupts, the backup data won’t corrupt along with it.

Health and Safety

It is very unlikely that computer equipment will be dangerous in itself; it can be used in ways that can be hazardous to the health of staff. Many office workers spend a lot of their time working at their desk, on a computer. Bad posture, incorrect positioning of equipment and susceptibility to repetitive

strain injury are health and safety risks that employers like Trinity Communications are required to take seriously. The health and safety, management of health and safety at work regulations, provision and use of work equipment regulations and the work place legislations act all legislate to the use of computer equipment and Trinity Communications will have to take these seriously or face penalties. Employers need to carry out regular workstation assessments to make sure that computer screens are at the right level etc. If an employer suffers from repetitive strain injury, they may be provided with ergonomic equipment.

Organisational Policies

Organisational policies that relate to the use of business information can help make sure that decisions affecting staff: are understandable and consistent, meet the legal requirements, take full account of their impact and contribute to productive working relationships. These policies help Trinity Communications help make sure that staff has guidance to help them comply with legislation – e. g. usage of customer data should work with the requirements of the Data Protection Act. These policies also make sure that Trinity Communications make consistent decisions which are important in internal communications.

Business Continuance Plans

These are steps that a company like Trinity Communications puts in place to make sure it is capable of surviving a worst-case scenario. One step in this programme might include making regular backups of its information. The business might consider environmental factors like accidents or natural

disasters like flooding or fire. As a result of this plan, employees may need to change the way they work – for example, storing information on a central server rather than on their personal hard drive.

Costs

Most businesses would see the benefit of implementing some, if not all of the measures listed. However, many aspects of information management can cost money, for example, while it may be desirable to store backup copies of electronic information on a remote server, a small business might not be able to afford this. When deciding what policies to adopt and measures to take, Trinity Communications need to consider the implementation and maintenance costs versus the benefits to the organisation. Some key considerations are: additional resources needed (would the business need to purchase new equipment or employ additional staff) and cost of the development (is there a solution already available or will the company need to develop it themselves, e. g. as an off the shelf product or a service). There are many consequences of increasing reliance on technology and increasing the complexity of that technology is that employees need to be trained to use the equipment and software required to do their job; this will increase the costs of increasing sophistication.