**Answers**

1. Foxhalls is a letting agency advertising and arranging property sales and rentals. The manager wants to ensure that they are complying with the Data Protection Act in relation to keeping personal data safe and secure.

 Gemma, an IT consultant, has been asked to advise the management on security issues. In particular she says that data should be encrypted when stored on their systems or when transmitted.

(a) State what is meant by the following terms with respect to encryption:

 Plaintext: [1]

The original message to be encrypted.

 Key: [1]

The piece of information needed to encrypt or decrypt data.

(b) Foxhalls store their data on encrypted hard disks. Explain how this helps to keep
their data secure. [2]

If a hard disk is stolen and not encrypted it can be read by the thief (1) if the disk is encrypted then it won’t be possible to read (1) unless the password / encryption key is known (1) the key to read the hard disk will only be remembered whilst the computer is being used. (1)

(c) Explain **one** advantage and **one** disadvantage of the use of strong encryption for communications. [4]

 Advantage:

Communications are more secure (1) which means that confidential information / personal information is less likely to be stolen (1).

 Disadvantage:

Communications can’t be read by police / security services (1) so they may find it harder to prevent crimes (1).

(d) The HTTPS protocol is used for secure communications between the company website and users.

(i) Describe the purpose of a communications protocol. [2]

It is a set of rules (1) for defining methods of data communication between different devices (1).

(ii) Describe how the HTTPS protocol operates to ensure secure data transmission over the Web. [4]

HTTPS uses asymmetric / public key encryption / cryptography (1).
SSL / TLS are encryption protocols (1).
A public key is used to encrypt data (1).
A private (secret) key is used to decrypt data (1).
The public key can be known by anyone (1).
The private key will be kept secret (1).

HTTPS uses SSL (Secure Socket Layer) or TLS (Transport Layer Security) protocol (1).

HTTPS facilitates an encrypted connection between a browser and a web server (1).

An SSL/TLS certificate can be used to authenticate the identity of a website (1).

(iii) Explain the purpose of a digital certificate in this situation. [2]

The digital certificate (SSL/TLS certificate) is issued by a certificate authority (1) which will verify that the domain name and key match. (1) It is also possible to verify the identity of the digital certificate owner (1).

(e) Foxhalls management are currently developing a website which will allow their rental customers to report problems, such as leaks, in their rental properties. Tenants will need to log in to the system before they can use it.

 Gemma has advised Foxhalls that they must only store hashed passwords for users in their database. Explain how the use of hashed passwords keeps data more secure. [4]

The password is run through an algorithm which will produce a hash (scrambled version) of the password (1). The hashes are stored on the database rather than the actual password (1). When the user attempts to log in, their password will be run through the hash algorithm (1) and then the hash of their password will be compared with the hash stored in the database (1). User passwords are therefore never stored on the database (1) so even if a hacker gets access to the database they won’t have access to the passwords (1).

 [Total 20 marks]