IT SECURITY POLICY

Aims

- to protect the company's digitised information assets from all threats, whether internal or external, deliberate or accidental
- to ensure continuity of information services by preventing breaches in the security of the company's information systems

Objectives

- information will be protected against unauthorised access
- confidentiality of information will be assured
- integrity of information will be maintained (i.e. safeguarding the accuracy and completeness of information by protecting against unauthorised modification)
- regulatory and legislative requirements will be met
- company requirements for availability of information and information systems will be met

Goals

- no unauthorised machine or person shall be permitted to gain access to the company network
- machines connected to the company network shall be used only by persons authorised to do so, and only for the purposes for which they are authorised
- no unauthorised software shall be permitted to run on machines connected to the company network
- data on machines on the company network shall be secured against unauthorised access, and against loss and corruption
- confidential data will also be secured in transit
- contingency and disaster recovery plans will be produced, maintained and tested
- services required by company users will be managed in such a way as to deliver maximum continuity and availability

Reviewed September 2021

Implementation

All of White Horse's IT systems are maintained and supported by external consultants and a contract exists with them for all IT services, including security and back-up.

- The entire system is protected through the use of Sophos anti-virus and firewall which continually updates.
- We also use the web security and control functions within our Sophos software to block "Adult and potentially inappropriate categories". A list of all the different categories that can be blocked is provided here: https://www.sophos.com/en-us/labs/web-control.aspx and is kept under constant review.
- The system is networked and access to the system is restricted via user name and password. There are different levels of access depending on roles and passwords and users are set up according by IT support according to instructions from senior White Horse staff.
- Remote access to the system is limited to senior White Horse staff
- Back-ups take place overnight and are streamed off-site to the IT consultants servers as well as on an internal server
- Learners are given clear instructions on induction as to acceptable use of the IT systems and are not allowed to access the White Horse system other than with permission of a member of staff and under supervision
- Student data is stored on a PICS database system which can only be accessed through a series of passwords by those authorised to do so. No data from this is distributed other than through the standard upload system to the ESFA.

A Mobile Technology and Social Media Policy is in place within White Horse Training a copy of which can be found on our website, in the resources section of the e-portfolio or is available from a member of staff.