Castleford Academy

E-Safety Policy

Version No:	Date Ratified:	Review Date:
2.0	14.10.2020	14.10.2023

Introduction

The curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. Teachers need to plan to integrate the use of communications technology such as web-based resources and email. ICT skills are vital to access life-long learning and employment. Technologies present risks as well as benefits. Internet/social networking use for work, home, social and leisure activities is expanding in all sectors of society. This brings pupils into contact with a wide variety of influences, some of which may be unsuitable. Unmediated Internet access through computers, telephones, ipads etc. brings with it the possibility of placing pupils in embarrassing, inappropriate and even dangerous situations.

Refer to Castleford Academy Safeguarding Policy.

Core Principles

- Guided Educational Use – curriculum internet use should be planned, task-orientated and educational within a regulated and managed environment.
- Risk Assessment – pupils must be protected from danger (violence, racism, exploitation) and learn how to recognise and avoid it.
- Responsibility – all staff, governors, external providers, parents and pupils must take responsibility for the use of the Internet.
- Regulation – in some cases eg. unmoderated chat rooms, immediate dangers are presented and their use is banned. In most cases strategies on access must be selected and developed to suit the educational activities and their effectiveness monitored.
- This policy is closely related to the guidance contained in;
  Keeping Children Safe In Education – statutory guidance to schools and colleges (DfE September 2019).
- With regard to Radicalisation via the internet and social media the academy fully adopts The Prevent Duty – departmental advice for schools and childcare providers (DfE June 2015).

Importance/Benefits of Internet Use

- Raise educational standards, promote pupil achievement.
- Support work of staff and enhance management systems.
- Part of the curriculum and a necessary tool in teaching and learning.
- Pupils are entitled to quality Internet access as part of their 21st century learning experience.
- Access to worldwide resources and experts.
- Educational and cultural exchanges between pupils worldwide.
- Facilitate staff professional development.
- Communication with external services.
- Exchange of curriculum and administrative data/sharing of good practice.

Ensuring Internet use Enhances Learning

- Internet access will be designed expressly for student use and will include filtering appropriate to pupils' ages.
- Pupils will be taught what is acceptable and what is not acceptable and given clear learning objectives when using the Internet.
- Internet use will be planned to enhance and enrich learning. Access levels and online activities will be provided and reviewed to ensure they reflect curriculum requirements and student age.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Student Evaluation of Internet Content

- Any user discovering unsuitable sites must report the address and content to; the Network Manager, a teacher or the Designated Safeguarding Lead as appropriate.
- The use of Internet derived materials must comply with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

Management of Email

- Pupils may only use approved email accounts on the academy system.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal details such as address/telephone number of themselves or others or arrange to meet anyone in email communication.
- Social email can interfere with learning and will be restricted.
- Email sent to an external organisation should be carefully written and authorised by a teacher before sending.

Management of the Academy Website Content

- The point of contact on the website should be the academy address, email and telephone number. Staff and pupils' home information will not be published.
- Use of photographs showing pupils and pupils' names will not be used on the website without parental consent.
- The copyright of all material must be held by the academy or be attributed to the owner where permission to reproduce has been obtained.

Social Networking
- Pupils will not be allowed access to public or unregulated chat rooms, social networking sites and forums.
- Pupils may only use regulated chat environments and forums – this use will be supervised, whenever possible, and the importance of chat room safety emphasised.

Managing Emerging Technologies
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the academy is allowed.
- Mobile phones will not be used during lessons (or the rest of the academy day) unless they provide a benefit to a student's education.
- The academy's video cameras may be used by pupils for educational use.

Authorisation of Internet Access
- All Internet access is monitored and recorded using electronic means.
- Inappropriate use of the Internet will be dealt with in accordance with the academy's Behaviour Policy.

Risk Assessment
- Some material available via the Internet is unsuitable for pupils. The academy will take all reasonable precautions to ensure such material is not accessed by pupils. However, it is not possible to guarantee that such material will never appear on an academy computer – Castleford Academy cannot accept liability for material accessed or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risk will be reviewed regularly.

Management of Filtering
- The academy will work in partnership with parents, the DFE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- Any Internet user must report unsuitable/illegal sites to the Network Manager (and the Designated Safeguarding Lead if necessary) immediately.
- The Network Manager will oversee regular checks to ensure that the filtering methods used are appropriate, effective and reasonable. Content is filtered using 'Light Speed' and 'Fortigate' and communications are monitored through 'AB Tutor'.
- If filtered websites need to be used by staff, they must inform ICT Technicians to have them unblocked for a set period of time (requests need to be approved by the Line Manager).

ICT System Security

- The academy's ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Files held on the academy's network will be regularly checked.
- Use of portable media such as memory sticks and CD will be reviewed regularly.
- Downloading of unauthorised files will be prohibited, and where possible blocked.
- Use of the academy's ICT systems will be subject to the Data Protection Act and the Computer Misuse Act.

Student, Staff and Parental Awareness

- All stakeholders will be made aware of this policy and how it relates to them.
- All staff will sign the Acceptable Use Policy.
- Pupils will be instructed in responsible and safe internet use before being granted access.
- Responsible use of the internet, including social networking will be discussed through the Computing curriculum, assemblies and PHSE.
- The monitoring of internet use is a sensitive matter – staff who operate monitoring procedures will be supported by the Network Manager and responsible Assistant Headteacher.
- Staff training in safe and responsible internet use and on the contents of this policy will be provided as required.
- A partnership approach with parents will be encouraged, with relevant information on issues covered by this policy made available.
- Cases of internet misuse and other disciplinary breaches related to the policy will be dealt with through the academy's Behaviour, Bullying and Safeguarding/Child Protection Policies, as appropriate. In cases of potential radicalisation/extremism The Prevent Duty will be implemented and could involve referral of individuals to the Prevent Duty Delivery Board and the Channel Panel.