Hopefields Education
E-Safety Policy

Introduction

Hopefields Education regards the online safety of the students as paramount. Students and vulnerable adults who attend the centre need the help and support of the centre to recognise and avoid on line safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression with the opportunities for creative activities and will be provided in the following ways:

- Key on line safety messages should be reinforced as part of a planned curriculum.
- Students should be taught in all lessons to be critically aware of the materials/content they access on line and be guided to validate the accuracy of this information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues.
- Students should be helped to understand the need for the *Student E-Safety Agreement* and encouraged to adopt safe and responsible use both within and outside the centre premises.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre- planned, it is best practice that students should be guided to sites checked as suitable for use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education and Training – staff and volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy.

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the centre E Safety Policy.
- All technical issues are dealt with by local IT company *Matrix Computers.*
-

- Appropriate security measures are in place to protect the servers , firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts which might threaten the security of the centre's systems and data. Secure E mails are used when communicating with professionals when appropriate. Password protection is used where sensitive information is transferred.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, however, staff , parents, carers and students need to be aware of the risks associated with publishing digital images on the internet. Hopefields will inform and educate users about the risks and will implement policies to reduce the likelihood of the potential for harm.

Written permission from parents/carers will be obtained before photographs of students/vulnerable adults are published on the Hopefields website, social media and local press.

Staff are allowed to take digital/photo images to support educational aims but must follow this policy concerning the sharing, distribution and publication of these images. Those images should only be taken on centre equipment, not the personal equipment of those staff.

Students/ vulnerable adults/staff/volunteers must not take, share, publish or distribute images of others without their permission.

Students/vulnerable adults names must not be used anywhere on a website or blog, particularly in association with photographs.

Students' work can only be published with the permission of the student and parents/carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive

- Kept no longer than necessary
- Processed in accordance to the data subject's rights
- Secure
- Only transferred to those with adequate protection
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on a secure password protected computers and other devices, ensuring that they are properly logged off at the end of the session in which they are using personal data.
- Transfer data using encryption and secure password devices.

Communications

Students/vulnerable adults are allowed mobile phones on site, but must lock them away in the Hopefields safe when they enter the site. Mobile phones are not allowed during contact time, but can be used during break and the first ten minutes of lunchtime.

A secure password means that students are not allowed internet access from the site server.

Users must report to the Directors if they are in receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Any digital communication between staff and students/ parents/carers (email, texts) must be professional in tone and content.

Students/vulnerable adults should be taught about online safety issues such as the risks of sharing personal details. They should be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

Social Media

With an increase in use of all types of social media for professional and personal purposes, it is important that staff are aware of what is appropriate to post on line. Details on the use of photographs/ videos and names/personal information is already previously stated in this policy. This also applies to students and the vulnerable adults who attend Hopefields.

Incidents

It is hoped that all members of Hopefields will be responsible users of digital technologies and understand/ follow this policy. However, there may be a time when infringements of the policy could take place, through careless or irresponsible or very rarely, deliberate misuse. In the event of suspicion, the following process should be carried out:

- Directors should be made aware.
- If a laptop has been used, this must be removed and if necessary, police involved.
- If it is an inappropriate site, the URL of the site containing the alleged misuse must be recorded and the nature of the content causing concern also noted. It may be necessary to record and store screenshots of the content on the laptop being used for investigation. These may be printed and signed (except in the case of images of child abuse).
- Once this has been completed and fully investigated, the Directors will need to judge what further action is necessary: Internal response/discipline procedures, Involvement of outside professionals (social workers, staff at host schools etc) Police involvement/action.
- If the content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately.
- Other instances to report to the police would include: incidents of "grooming" behaviour, the sending of obscene materials to a child, adult material which potentially breaches the Obscene Publications Act, criminally racist material, promotion of terrorism or extremism, other criminal conduct activity or materials.
- Staff must isolate the laptop in question. Any changes to its state may hinder a later police investigation.

Actions and Sanctions

It is more likely that Hopefields Directors will need to deal with incidents that involve appropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner. Incidents of misuse will be dealt with by warnings to staff members (if appropriate) and referrals to senior management/parents/carers/Police/ removal of internet access/suspension/exclusion depending on each individual case. Notes will be made on staff records and student/vulnerable adult CPOMS record as appropriate.