**SENSE COLLEGE - E-SAFETY GUIDANCE**

**Introduction**

This guidance provides a brief summary of the actions that a user may take to protect themselves when using IT and the internet. This document should be read as a general principles summary, rather than an exhaustive guide.

This guidance should be read alongside the Sense College E-Safety Procedure, which should be applied at all times. This document also relates to other Sense policies and acceptable use agreements.

**Working with Students/Supported Individuals**

All staff that support students/supported individuals to access IT or the internet have a responsibility to ensure that they are used responsibly, appropriately to the session or personal development goals, and above all, safely.

Some students/supported individuals may not fully understand the concept of ‘safety’, so a number of ‘rules’ can be provided to help guide and support this.

**Electronic Communications**

This includes email, chat rooms, social networking sites, instant messaging, forums and the like. Apart from email, all of these are prohibited to staff unless permission is given by the College SMT and/or it is related to business use/accounts.

Students/supported individuals may be allowed to use these services on an individually risk assessed basis. Students/supported individuals should aim to:

* Only communicate with people they know, and never arrange to meet anyone following any online contact
* Report attempts at communication from people they do not know to a member of staff
* Use polite, appropriate language at all times
* Never reveal any personal details such as phone numbers, addresses, dates of birth – of either themselves or anyone else
* Should never exchange files such as photos using these services
* When using a social networking site or similar service, students/supported individuals should be encouraged to use access management tools available to prevent anyone from making contact with them who is not on their ‘safe’ list
* Bullying and other forms of abuse can take place through these systems; students/supported individuals should report this to an appropriate person (such as a member of staff) as soon as possible.

In the case of email:

* Any emails received from an unknown person should be deleted without opening
* It should be understood that email is not secure and can be read by design or accident
* Attachments to messages should be treated with extreme care, even when they appear to be from a known person. Executable attachments (attachments that include files ending in .exe, .com, .vbs, and .js) should be deleted. Attachments from unknown sources should always be deleted
* Any offensive email should be reported as soon as possible
* The forwarding of ‘joke’ or ‘chain’ email is not allowed

**The World Wide Web**

The web is one of the most powerful tools available for educational use, however it must be used appropriately and carefully to get the best out of it. When using the web with students/supported individuals for academic purposes, staff should consider:

* Reviewing with students/supported individuals the content of the Acceptable Use Agreement prior to starting the course/activities, to remind them what is considered ‘acceptable use’
* Should verify that any information or media downloaded does not break copyright or intellectual property laws
* Setting clear outcomes from the use of the internet
* Suggest a list of search terms or websites
* Provide guidance on evaluating the quality of information found
* Students/supported individuals or staff should report the accidental access of inappropriate materials so that access can be blocked
* If a website of a legitimate nature is blocked this will be unblocked after being checked
* Do not use the college computer systems for financial transactions of any kind (for staff, business use is permitted if part of role). If this is done, the college will not accept any liability for any resulting losses

**Computer Security**

The managed computers within the college have anti-virus software installed as well as other protective mechanisms.

Computers used within the college ‘perimeter’ are also subject to filtering; filtering can ensure that all undesirable content is filtered out. Computers used outside the college are at increased risk, but no computer can ever be said to be 100% secure and protected from all forms of hacking, viruses or other mal-ware. Care should be taken to avoid falling victim to identity theft, fraud or other threats.

**References and Information Sources**

The following websites provide further sources of information and additional details to support the references made within this guidance and the E-Safety Procedure.

It is to be noted that some of these websites guidance may be aimed at schools, therefore may need some interpretation for our environment. Please bear in mind that these websites are provided for information only and are not an alternative to following the college’s own procedures and policies.

* BBC - The WebWise Online Course; Keeping safe

<https://www.bbc.co.uk/programmes/p00j17gt>

* The National Archives

[http://webarchive.nationalarchives.gov.uk/20101102103639tf\_/http://www.nextgenerationlearning.org.uk/safeguarding](http://webarchive.nationalarchives.gov.uk/20101102103639tf_/http%3A//www.nextgenerationlearning.org.uk/safeguarding)

* Childline

<https://www.childline.org.uk/>

* Child Exploitation and Online Protection Centre

<https://www.ceop.police.uk/safety-centre/>

* Childnet Internation (formally known as Kidsmart)

<https://www.childnet.com/>

* East Midlands JISC group – the 5 ‘T’s of E-Safety

<https://www.em-esafetyproject.co.uk/>

* Grid Club and the Cyber Café

<https://gridclub.com/>

* Internet Watch Foundation

<https://www.iwf.org.uk/>

* Kent Online Advisory Service, provided by Kent County Council

<http://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety>

* NSPCC

<https://www.nspcc.org.uk/>

* Think U Know

<https://www.thinkuknow.co.uk/>

* Virtual Global Taskforce

[https://nationalcrimeagency.gov.uk/virtual-global-taskforce/Global Taskforce - National Crime Agency](https://nationalcrimeagency.gov.uk/virtual-global-taskforce/Global%20Taskforce%20-%20National%20Crime%20Agency)