Appendix 1

Sense College

Staff Acceptable Use Agreement

This Acceptable Use Agreement is intended to ensure that:

- You will be a responsible user and stay safe when using the internet;
- You will support learners/supported individuals appropriately;
- You will use computers and digital technologies properly for educational, personal and recreational use;
- You will take care and help to protect college systems and users from accidental or deliberate misuse or harm;
- You will follow Sense's policies, procedures and Sense College's e-Safety Policy.

ACCEPTABLE USE AGREEMENT- DECLARATION

Name:	

I have read the Sense College e-Safety Procedure and I understand that:

- I will comply with the e-safety procedure and Sense's Acceptable Use Policy and understand that any failure to do this may result in disciplinary action that could lead to dismissal.
- The college (and Sense) owns the IT systems and I understand it is a criminal offence to use a computer system for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I will not give my user account password to anyone else and I will only access the college computer systems with my own username and password. I will inform IT Helpdesk if I believe my Sense password has been compromised and College SMT if my Databridge password has been compromised.
- I will not access, or attempt to access other people's files.

- I will not modify or circumvent system settings or software, attempt to install software or install and/or modify hardware without seeking help from IT staff.
- I will virus scan all media brought in from outside college.
- I will not send offensive, unnecessary or inappropriate email.
- I will not access pornographic or otherwise offensive or inappropriate web sites.
- I will not access extremism or radicalisation or other associated inappropriate web sites.
- I will inform College SMT and/or IT Helpdesk if I accidentally access inappropriate material.
- I will observe copyright and intellectual property rights and law.
- I will report any incidents of concern regarding child or adult protection and safeguarding to the Designated Lead or VP responsible for Safeguarding. This will be reported using the 'concern' procedure.
- I will ensure that all communications with learners/supported individuals are compatible with my role and meet the requirements of the college polices/procedures.
- I will follow the data protection policy and will ensure that personal data is kept secure and is used appropriately, whether in college, taken off college premises or accessed remotely. In understand this includes the use of photographs and videos.
- I will promote the concept of 'e-safety' when working with learners/supported individuals.
- I understand that random checks of files and the log of visited internet sites will be undertaken.

Signed:		Date:	

Appendix 2

Sense College

Student/Supported Individual Acceptable Use Agreement

This Acceptable Use Agreement is intended to ensure that:

- You will be a responsible user and stay safe when using the internet;
- You will use computers and digital technologies properly for educational, personal and recreational use;
- You will take care and help to protect college systems and users from accidental or deliberate misuse or harm.

ACCEPTABLE USE AGREEMENT - DECLARATION

Name:		MCA Capacity / Support Need:	

I will use the college systems in a responsible way, to ensure that there is no risk to my safety or the safety and security of other users or college system.

For my own personal safety:

- I know that Sense College will monitor/look at my use of the computers, equipment, internet and digital communications.
- I WILL be aware of 'stranger danger' and know how to stay safe when I am communicating online.
- I WILL tell staff if I see anything that is unfriendly or that makes me feel uncomfortable or upset.
- I will tell staff if some online harasses me or wants to talk about rude things.
- I will NOT give personal information about myself to anyone online.
- I will NOT give my username or password to anyone else.
- I will NOT fill out forms or enter my information to win free things

For the safety of college and other people:

- I WILL tell staff straight away about any damage or problems with the computers and equipment.
- I WILL check with staff first before I:
    - Use social media sites
    - Download or upload any files
    - Open emails or messages from people I don't know
    - Use the computer for personal tasks
- I will NOT access or look at anything that is illegal or inappropriate or that may upset other people.
- I will NOT use anyone else/s username or password.

I understand that everyone has equal rights to use technologies and resources:

- I WILL only use the internet and technology equipment for college work.
- I will NOT use the college internet or equipment for shopping, online gaming, gambling or video sharing (e.g. YouTube) unless I have permission from a member of staff to do so.
- I will NOT copy of files (including music and videos)

I will act appropriately and respect others:

- I WILL respect other people's work and things.
- I WILL be polite and responsible when I communicate with others.
- I will NOT use strong, aggressive or inappropriate language.
- I will NOT take or send images of anyone without their permission.

I am responsible for my actions:

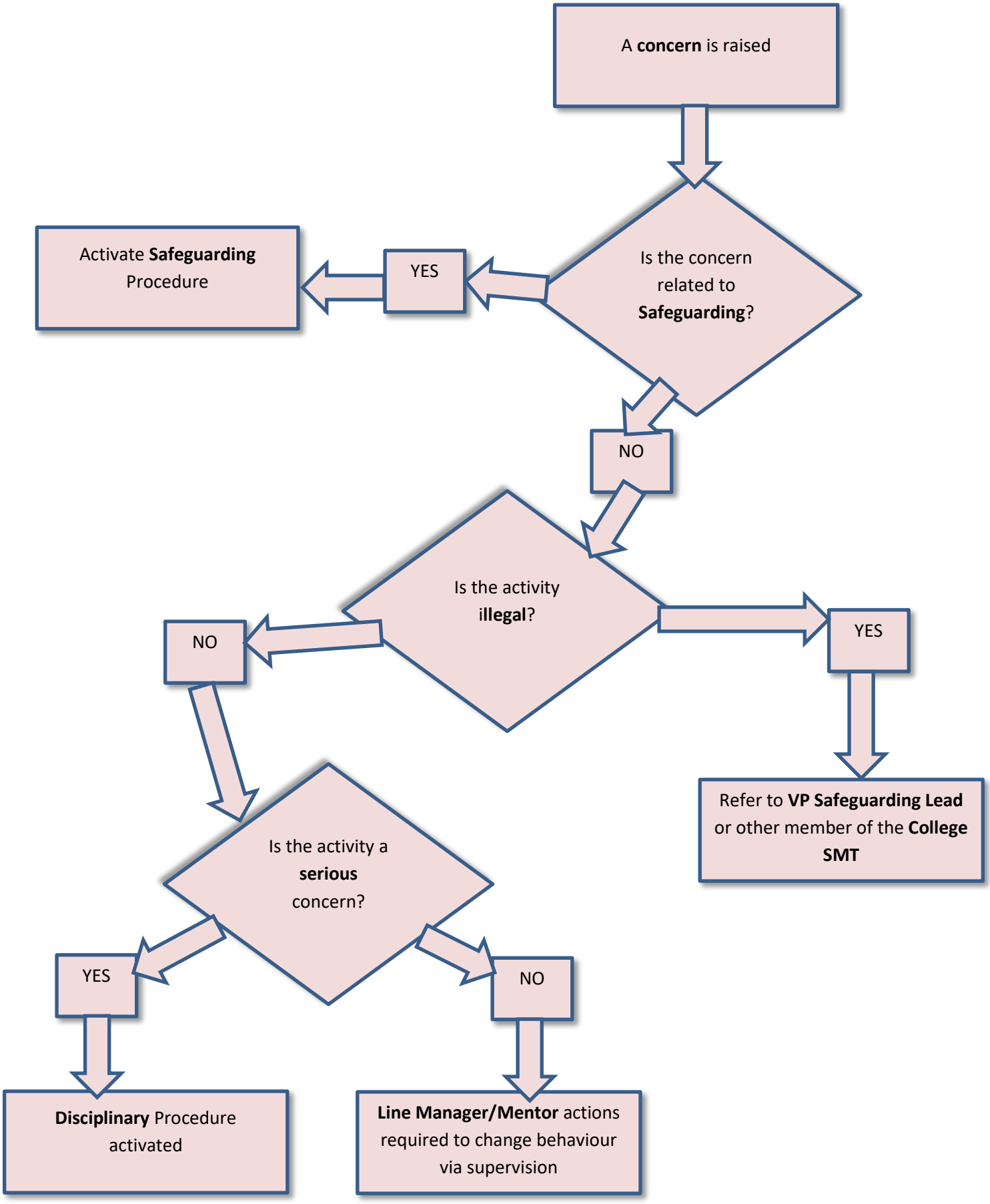
- I know that if I do not follow these rules, I will not be allowed to access the internet or technology equipment and may also put my college placement at risk
- I know that if I am involved in any incident or inappropriate behaviour, safeguarding procedures might mean that further action could be taken.

Please note below any other discussions, explanations or agreements that have taken place

Signed:		Date:	
*If proxy – state name/relationship to student:			

Appendix 3

SENSE COLLEGE - E-SAFETY FLOWCHART



Appendix 4

SENSE COLLEGE

STUDENT/SUPPORTED INDIVIDUAL'S CREDENTIALS – SUPPORT BY STAFF

Guidance

This guidance provides a summary of the requirements and actions that staff should take when supporting students/supported individuals to login to college computer systems requiring usernames and passwords to access them.

The aim of this process is to protect staff when using IT and the internet, particularly at those times when there is a need to know the login credentials provided for students/supported individuals use and to protect the students/supported individuals themselves from misuse/abuse. 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 Policy, 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 and 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.

Although a student/supported individual may be provided with their own Sense credentials and be able to access and use college computers and internet, they may require support to be able to remember and enter login usernames and passwords into the systems.

An allocated/dedicated member of staff, such as a mentor or personal tutor, who supports the student/supported individual with IT/computer access may need to have the knowledge of the student/supported individual's password, but they must never use these credentials for their own use or to mask other activity.

If a breach of this process is discovered and a staff member is found to be inappropriately utilising a student's/supported individual's login credentials, they will be subject to Sense's Safeguarding processes and disciplinary procedures.

Support Knowledge of Login Credentials – Staff Declaration

Any staff member that has the knowledge of another person's Sense login credentials (including username, password and in some cases a safe word) – particularly that of a student/supported individual – must complete the declaration below.

I understand that as part of my role and the support I provide to students/supported individuals, I may be required to have knowledge of individual's own Sense login credentials – such as username and password.

I will not disclose any information, usernames and passwords that I may have knowledge of, to anyone else.

I will not utilise anyone else's login credentials for any other purpose than to support the individual user that the credentials belong to.

I will not utilise anyone else's login credentials to undertake any work or personal use, or to mask other activities/uses.

I understand that if I breach this declaration and the associated E-Safety Policy I will be subject to Safeguarding processes and Sense's disciplinary processes.

Signed:		**Date:**	
Name:			

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

- 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/

- 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/