Sense College - Operational Strategy

E-Safety

Information and Process

Outcomes

In order to safeguard all college learners/supported individuals, staff and stakeholders visiting the college sites, the purpose and aims of e-Safety for the college needs to be clear:

- To ensure that all parties are aware of e-Safety and internet security measures;
- To ensure that all learners/supported individuals and staff are protected from inappropriate material and contacts (as far as is practical or technically feasible);
- To ensure that college safeguarding procedures are applied when using IT/technologies (Note that this includes carrying out the Prevent Duty);
- To explain what the responsibilities of staff, learners/supported individuals, and stakeholders are within the e-Safety strategy and to provide information on what acceptable use is and what it is not;
- To ensure that learners/supported individuals and staff concerns about e-Safety are taken seriously and acted upon appropriately;
- To support the informed decision-making skills of learners with parents/carers and staff support;
- To ensure that staff have the skills required to seek and respond effectively to the strategy requirements;
- To work to the principles of the SEND Code of Practice (2014), the Mental Capacity Act (2005) and the Equality Act (2010) and other current legislation for e-Safety and technology in liaison with external stakeholders support, such as NATSPEC TechAbility;
- To ensure reviews of the strategy inform quality improvement.

For the college E-Safety Strategy to be effective, it is important that all users are clear about its purposes and understand the processes, protocols and outcomes; and above all, perceive it as an effective and supportive mechanism for raising standards, improving safeguarding and learner/supported individual journeys/experiences. Staff will monitor the effectiveness of the strategy and contribute to its development through meetings and the college's quality assurance systems.

Who is this strategy for?

This strategy is for all Sense College staff, in addition to:

- Learners funded by the ESFA (Education and Skills Funding Agency);
- Supported individuals using college sites/centres for day services;
- The parents[1]/families who advocate and sign for Individuals that Sense supports;
- All College agency staff and volunteers;
- Governors;
- Stakeholders, including visiting Sense staff, trainers and organisations who may use the college network;
- College Senior Management Team.

Staff from the wider Sense organisation and IT teams may find this strategy helpful too.

What is this strategy about?

Sense College recognises the benefits and opportunities which technologies can offer to teaching, learning and assessment. However, the accessibility and global nature of the internet and the different technologies available mean that we are also aware of potential risks and challenges associated with such use.

The college wants to encourage, promote and support the use of technologies in a safe way and this strategy is not intended to limit the use, but to create a culture where people can safeguard themselves. The college recognises the use of technology to support communication, independence, living skills, education and vocational/careers learning.

The College approach is to implement appropriate safeguards within the college while supporting staff and learners/supported individuals to identify and manage risks independently and with confidence. We believe this can be achieved through a

[1] • Throughout this document, in the context of the strategy, the term ‘parent(s)’ is inclusive of parents, carers and/or family members who act as next of kin and guardian to the individual/learner and who provides daily support/advocacy.

combination of security measures, training, guidance and the implementation of our policies/procedures and strategies.

Definitions

Staff – All staff, volunteers and placement students/supports are subject to this strategy. A failure to agree to abide by this strategy and the accompanying Acceptable Use Agreement will result in the individual not being granted access to the college's computer system and internet connections; this will be referred to the individual's line manager. Failure to follow this strategy may also lead to disciplinary action.

Learners – All learners and supported individuals enrolled at the college. Learners/supported individuals issued with individual user accounts will have the Sense College Learner Acceptable Use Agreement explained to them. When supporting learners/supported individuals, staff should maintain the college E-Safety Strategy and Acceptable Use Agreement and where possible, work to aid the learners' knowledge of this strategy and e-Safety in general.

The Internet – To include all services provided via the communication tool known as 'The Internet' (this includes, but is not limited to the world wide web, email, FTP (File Transfer Protocol), newsgroups, communication services such as MSN, Yahoo etc) and all services of web based providers such as social networking, video and other media streaming and downloads. This is not an exhaustive list.

E-Safety – This is the concept of 'staying safe online' and is essentially about the things a user can do to protect themselves. The concept is very similar to staying safe in the real world and could be summarised as being aware of potential risks and the simple actions that can be taken to reduce these risks.

Mobile Devices – Any portable devices that has radio frequencies, Wi-Fi or any other ability to communicate with networks or other devices. This includes mobile phones and other internet capable devices such as iPods, iPads, tablet PCs, netbooks and laptops.

Contents

Part Seventeen: Handling Complaints and Breaches of Procedure

Part Eighteen: Acceptable Use

Part Nineteen: Third Party Account Access

Part Twenty: Purposes of Safeguarding and Prevent Duty

Quality Assurance

Conclusion

Appendices

Appendix 1 – Staff Acceptable Use Agreement Declaration

Appendix 2 – Learner Acceptable Use Agreement Declaration

Appendix 3 – E-Safety Flowchart

Appendix 4 – Learner/Supported Individual Password Support by Staff – Guidance and Declaration

Appendix 5 – E-Safety Guidance

Overview

Introduction:

Purpose of the Strategy

Sense College is committed to providing an outstanding learning environment which ensures all our learners/supported individuals and staff can engage with the use of technology and access the internet safely.

This document details Sense College's processes governing the use of computers and other related systems within the college, as well as the information stored and processed on them, both within Sense College and also in other locations when removed by staff from the college. It also covers the use of mobile devices such as tablet computers and mobile phones.

This procedure applies to all staff and learners/supported individuals of Sense College, who must read and then sign the Acceptable Use Agreement – there is one for staff (**Appendix 1**) and a separate one for learners/supported individuals (**Appendix 2**)

Background and Need

In recent years the use of IT and technology in Sense College has increased dramatically and the way the internet is used is now very different. This strategy is continually under review with the goal of making provision within the strategy for new emergent services and new uses of the internet and other IT/technology systems. t is important to note that this strategy is a superset of Sense's other policies and staff IT acceptable use policy.

Sense College has a Vice Principal responsible for safeguarding, who is also a Designated Lead/Person. Note that for the purposes of discharging the Prevent Duty and to maintain the highest standard of safeguarding generally, this procedure is directly linked to the Safeguarding Policy as shown in the e-Safety flowchart (**Appendix 3)**.

This e-Safety Strategy and the associated acceptable use agreements have been written and produced by the college, using former advice from JISC, NATSPEC and other stakeholders.

Sense College recognises the enormous benefits to be derived for both staff and learners/supported individuals from the use of IT, however there are risks and concerns that must be considered. The college aims to educate staff and learners / supported individuals about e-Safety but this must be a collaborative effort to enable an organisation wide response. Using IT and the Internet is part of the college's curriculum and is integrated into many subjects and contexts.

Due to the fact that we have internet access via every computer in the college (as well as mobile devices) there is a need for everyone to be familiar with appropriate and best practice when using the internet. Staff must remain vigilant and focussed on the needs of learners / supported individuals and the business of the college, whilst at the same time ensuring that the system is responsive and useable. All staff and learners / supported individuals (where appropriate) are provided with an individual user account to access the computer systems.

This strategy aims to help everyone understand what is acceptable use (what is appropriate and what is not). All persons using the college computer systems and internet connections must read and comply with the strategy. All users must also sign an agreement / declaration (**Appendix 1 and/or 2**). This is an important undertaking, as misuse of the college systems could lead to disciplinary action; this could range from the loss of internet access to dismissal for gross misconduct. If this strategy is breached, it could be the staff member, not only the college, that is held accountable for any resulting legal action. An example could be copyright violation – the downloading of copyright infringing films, software or music being possible breaches.

The college will operate various technological systems to assist in the maintenance of this strategy; this includes monitoring and filtering systems. Such technological systems are not a complete solution and will only be effective when combined with organisation wide commitment.

Associated Policies, Procedures and Strategies:

This e-Safety Strategy should be read alongside other relevant Sense Operational policies, procedures, strategies and guidance, as detailed below:

- CE01 Complaints Policy
- CE02 Data Protection Policy
- OS07 Youth Produced Sexual Imagery Guidance
- OS11/OS12 Safeguarding Procedures and Guidance
- OS26 Social Media Procedure
- HR08 Disciplinary Policy
- HR22 Social Media Policy and Procedure
- Staff Handbook
- ICT 008 Password Guidance
- ICT010 Social Media Safety Guidance
- Sense College - Tackling Extremism and Radicalisation Strategy
- Sense College - Anti-Bullying Strategy
- Sense College - Digital Capabilities and Wellbeing Strategy

Legislation and Regulation:

- Computer Misuse Act 1990
- Communications Act 2003 – including Telecommunications Act 1984
- Protection of Children Act 1999
- Copyright, Designs and Patents Act 1988
- Regulation of Investigatory Powers Act (RIPA) 2000
- Data Protection Act 2018
- The Prevent Duty – Counter-Terrorism and Security Act 2015
- Keeping Children Safe in Education (KCSIE)

Practice

Part One: Security

Appropriate security measures will be taken, which includes the use of enhanced filtering systems, to provide the protection of firewalls, servers, routers, workstations and the use of safe and secure passwords etc, to prevent accidental or malicious access of college systems and information.

Part Two: Filtering

In addition to the Sense organisational anti-virus and filtering system provided by Sophos, the College also uses an intelligent web content filtering and monitoring system called Smoothwall Secure Web Gateway, which has a bridging mode that dynamically analyses, understands and categorizes all web content requested by users.

The Secure Web Gateway provides:

- Protection from pornography and objectionable content
- Controlled access to non-work-related sites, such as news, sport, travel and auctions
- Protection from web-borne spyware, malware and browser exploits
- Reporting on internet behaviour and resource utilisation
- User authentication and filtering policies based on group membership
- Bridge mode operation

The college subscribes to this system for a ‘blocking service’ that aims to identify inappropriate content to prevent staff or learners/supported individuals from accidentally accessing offensive or otherwise inappropriate content. Whilst the college has taken reasonable action to prevent access to inappropriate content is should be noted that no such system is perfect and will on occasion both allow access to inappropriate material and block access to legitimate material. If a user accidentally accesses inappropriate

material they should inform the SMT designated lead for IT via emailing college.smoothwall@sense.org.uk so a block can be manually introduced. No individual will be punished for accidentally accessing inappropriate materials; such accidental access is clearly demonstrable in the internet logs created by the Smoothwall system. If a staff member requests a website to be unblocked this will only be done in the case of a clear business need and only when authorised by a member of the College SMT.

Should a member of staff or a learner/supported individual have another reason, research based or strong business case to be accessing extremist materials normally disallowed under the Prevent Duty, this should be authorised in writing by a member of the College SMT.

Part Three: Monitoring and Reporting

The Smoothwall Secure Web Gateway utilised by the college also provides live monitoring and subsequent reporting for all internet use, accessed by either college owned systems and devices or Bring Your Own Devices (BYOD) owned by individuals that use the Sense college Wi-Fi.

The core features of the monitoring system are:

- Content Aware Analysis
  Identifies and filters brand new web content in real time, long before the URL lists

- Gateway Anti-Malware
  Protects the network from web borne malware attacks

- Limit Bandwidth Use by Policy
  Limits can be set for bandwidth use by user, content type, time or locations

- Social Media Controls
  Controls to ensure that social networks are used productively

- ‘Who, What, Where, When’ system policies

  The ability for the college to build its own set of filtering, category, time, location and user controls, depending on individual requirements or protection

- Level 7 Application Control

  The ability to control non-web traffic, such as Skype and Bit Torrent (open file sharing platform)

- Social Media Controls

  Enable the productive use of social networks

- Anonymous Proxy Blocking

  To prevent circumvention of our e-Safety Strategy and acceptable use agreements

- Reporting Suite

  A range of reporting options to provide real-time alerts, requests and monitoring, as well as scheduled reports on activities and/or breaches

Monitoring of both network and internet activity will take place in a routine way. Random checks of files on the system may also be undertaken to both check that inappropriate material is not being stored and to control excessive use of the system.

Specialist software will be used to help detect trends in internet use and to monitor excessive use. By using this software it will be possible to tell who has accessed what materials, from which computer, when they accessed the site and how long there were connected for. Internet access logs will be reviewed by the college senior management team should a concern be raised, or periodically in the form of an audit as part of the college’s quality assurance processes.

Targeted monitoring will only take place when a member of the College SMT authorises it as part of an investigation. A line manager may request an internet access log for a member of staff under their direct line management if required for an investigation, by approaching the SMT appointed person. Whilst this is at the discretion of the manager, they must be able to justify this course of action.

Note, that in order to maintain the Prevent Duty, it is possible that should the Police contact the college for logs of visited websites (by any member of staff or any learner / supported individual); they will be shared with the Police at the discretion of the Executive Principal.

Where an e-Safety incident is reported to the college (whether by system alert/reporting or via an individual), this matter will be dealt with very seriously. The college will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring.

If a learner/supported individual wishes to report an incident, they can do so to any member of staff or the centre manager.

Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible, as well as their Education Services Manager/Deputy Designated Lead or a member of the College Senior Management Team.

Following any incident, the college will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident.

Serious incidents will be dealt with by senior management, in consultation with Sense HR and other appropriate external agencies, in accordance with Safeguarding policies.

Part Four: User Accounts

All staff will be allocated a personal user account to provide them with access to the college systems. No staff member should access or attempt to access the system with anyone else's account. If a member of staff accesses files that do not belong to them or they are not granted access, they should notify the IT Helpdesk and College SMT as soon as possible.

Learners/supported individuals will also be provided with a Sense account if appropriate and required.

There is no circumstance where a member of staff should give their username or password to anyone else. As the account is in the individual staff member's name, any misconduct detected on the account is technically their responsibility. If any member of staff feels that their password has been compromised, they should inform Sense IT Helpdesk as soon as possible. Any attempt to log into the system with any other account other than an individual's own account will lead to disciplinary action.

The only exception to this is where tutors or keyworkers need to support a learner/supported individual to access their account and as such needs to know/keep a record of the password in order to enable them to remind a learner/supported individual what their password is. For this purpose, separate guidance and a staff declaration form will be used (**Appendix 4**). If a learner/supported individual is able to remember their own password, or an alternative accessible login format is activated for them, then it is not appropriate for any staff member to know it.

Any staff member who uses a learner's account to conceal or attempt to conceal their own use of the internet or computer system more generally, will be subject to a gross misconduct disciplinary, as such an action will be treated as fraud.

Part Five: Use of Email and Internet

Sense College uses the sense email system for both internal and external use. Email must be used in a professional manner and with the same care and consideration as any other written medium.

Use of the college email system does not mean that messages transmitted from the college system are authorised by the college. Email should not be thought of as 'private'; it can be intercepted and read easily, either by design or accident.

Users must ensure that like any other form of communication, emails do not contain statements or inferences which could be interpreted by any recipient as disablist, sexist, racist, harassing, libellous, extremist or otherwise liable to damage Sense College or Sense's reputations. The sending of offensive or inappropriate emails will result in disciplinary action.

No user should attempt to send a message of any kind under a false or assumed name. Users should be mindful that anything sent out of the college email accounts will be traced back here. Users who receive abusive or otherwise inappropriate messages or material must inform line management as soon as possible.

Users should avoid all non-work related 'forwarded' emails such as those including jokes and 'chain letters'. Unnecessary messages not only deplete system resources, but can also annoy the recipients and give an unprofessional image of the sender and the college. Users should only send or copy messages to people whom they are really relevant.

File attachments should only be sent when absolutely required; often in the case of internal messages it is possible to state the location of a file on a shared drive. Any files received with email should be treated with care. Due to the increase in viruses that spread via email, it is a good idea to delete without opening all messages that come from an unknown source, especially if they have an attachment. Executable attachments of a non-business or unsolicited nature must not be opened or forwarded by any user. Executable files commonly end with .exe, .com, .vbs and .js. It is a good idea to not use the preview pane in Outlook; this prevents certain viruses from opening automatically. If a 'virus warning' from our anti-virus software is seen, this should be reported to the IT Helpdesk.

Users are to be aware that internet communications are not private; all email and other messages can be disclosed to law enforcement without the consent of the sending or receiving party.

Access to the internet is provided primarily for research and communication purposes and use for teaching support. All users have a responsibility to maintain and enhance the college's public image and to use the internet productively and in a professional manner.

The use of the internet covers all services, including but not limited to, the World Wide Web, email, mobile apps, Facetime, Skype etc.

The intended uses of the internet for staff are, email access, web based research for business and staff development purposes. However, as the College is an educational establishment that is committed to lifelong learning and development for all, staff internet access is not entirely limited to work related material. This should be considered a privilege and not a right and will be withdrawn if abused. Computer use is encouraged for staff development purposes. Staff can have internet access for a limited non-business use outside of their working hours or unpaid breaks, providing those who need to work do not require the computers/laptops/tablets. Staff that access the internet are still representing the college even when they are accessing the internet for non-business purposes. It is important to reiterate that access under this section of the strategy may be withdrawn if abused. Disciplinary action will be taken if excessive or inappropriate use is detected on a staff members account.

The internet must be used in an ethical and lawful manner. Any user found accessing pornographic, hate or other offensive material will have breached this strategy and the acceptable use agreement, and as such will be subject to disciplinary action. If illegal activity is detected then the police may be informed. If any activity is detected that puts other users at risk, the safeguarding policy will be activated and the Designated Lead informed.

The internet connection is filtered, but it is not possible to ensure that all inappropriate material is inaccessible from the college. Should users access hate, radicalising or other inappropriate material commensurate with the definition in the Prevent Duty (whether by accident or deliberate means), it will be detected by the Smoothwall system and routine log generation. A review will then be undertaken by the College SMT and/or IT Team and may then be followed up and treated as a safeguarding incident if deemed appropriate.

Use of the internet must not disrupt the internal network or any systems external to the college. It is not permitted to use any kind of hacking or cracking tool, attempt to decode passwords or other protected information, attempt to circumvent or subvert any security systems or engage in any activity that could harm systems or data. It is not permitted to

use any form of VPN (Virtual Private Network) or other ‘tunnelling’ tool to make a connection to another computer or system outside of Sense College network that in any way bypasses our firewall without the express prior written permission by College SMT and IT Team.

The college network / computer systems / internet connections must not be used for political purposes or to gain commercial or personal profit or advantage. This includes the use of buying and selling websites and services such as auction sites – unless authorised by SMT as part of college enterprises.

If any data is needed to be brought into college, it must be virus scanned before use. Any files received with email or downloaded from the web must be virus checked before use. The anti-virus software is updated regularly so we should be able to detect and eliminate all but the very newest viruses. If learners/supported individuals need help with virus scanning any media they should ask staff. If staff need help with virus scanning any media they should raise a request with the IT Helpdesk. If anyone is experiencing any unusual computer activity, report it to the IT Helpdesk as it could be symptomatic of a virus or other ‘malware’. IT/internet users should not load any data of a non-business nature into the college computer system by any means.

Part Six: Use of Personal Information

Personal information is information about a particular living person. Sense College collects and stores the personal information of learners/supported individuals and staff in line with work processes, such as names, dates of birth, email addresses, contacts, assessed materials and so on. The college will keep all information safe and secure as per strategy/policy/procedure and will not pass it on to anyone else without the express permissions as appropriate.

Please see CE02 Data Protection Policy and the OS08 Handling Information Guidance for further details.

No personal information will be posted or listed to Sense's website without appropriate permissions and consents being in place.

Only names and work email addresses of (senior) staff will appear on the Sense website.

Staff must keep learners'/supported individuals' information safe and secure at all times. When using an online platform, all personal information must be password protected. No personal information of individuals is permitted offsite unless the member of staff has the permission of Senior or Executive Management.

Every user of IT facilities has to have their own login username and password, and is required to log off on completion of any activity, or where they are physically absent from a device, to prevent any unauthorised view or copying of material/information.

All college mobile devices such as laptops, tablets, iPads, USB's (containing personal data) are required to be encrypted and password protected.

Where the personal data is no longer required it must be securely deleted in line with the General Data Protection Regulation (GDPR).

Part Seven: Use of Images and Video

The use of images, photographs or videos is popular in teaching and learning and should be encouraged where there is no breach or copyright or other rights of another person. This will include images downloaded from the internet and those belonging to staff and learners/supported individuals.

When images/photographs/videos are being selected, care should be taken to ensure that those chosen, suit the individual needs of each user and purpose. Images, photographs and videos should be appropriate to both the developmental level of the learner and to the subject area of teaching and learning.

No image/photograph can be copied, downloaded, shared or distributed online without the individual's permission. The relevant forms to gain this permission are available on IRIS, as well as the consent given within the college learner enrolment form.

Photographs of activities on the college premises should be considered carefully by Education Services Managers before being published. Managers and staff should consider the appropriateness of the image and what can be gained from sharing it in this way. Part of this consideration should also include ensuring that the appropriate consent has been given for all individuals visible in, or linked to, the image.

Video can be used in creative or media based sessions as well as training. In each case the staff member must take responsibility for the appropriate use of video material. Increasingly we are making use of video for progression recording and training purposes. The purpose of this is to show progression visually without the need for long written accounts and to use for internal training purposes or to spread best practice. It is not acceptable for staff to place video featuring learners/supported individuals on YouTube accounts or other services.

A code of conduct for using video must be adhered to:

- All recordings should be consensual;
- At least two members of staff should be present during the session;
- The session should have a clear beginning and end, and all persons should know when the camera is recording;
- No video should show a learner/supported individual or staff member in an inappropriate, degrading or improper situation;
- Video should not be used to demonstrate personal care procedures;
- All use of video must adhere to child/adult protection safeguarding policies and procedures;
- There must be a clear and documented purpose for the recording;
- There must be a named member of staff responsible for the recording session;
- Video must be stored according to the data protection policies;
- Video must not be removed from the college in any form unless explicitly authorised by a member of the College SMT.

The only exceptions to the above video code of conduct are:

- The distribution of pre-authorised creative arts productions which may leave the college without individuals approvals;
- The video recordings for RARPA (Recognising And Recording Progress and Achievement) that are stored on college owned equipment such as laptops, and portable hard discs may be removed by the tutor/staff member responsible for them, at the risk of the staff member individually, who will be held accountable in the event of their loss.

Part Eight: Use of College Equipment

The college issues laptops, cameras, video cameras, external hard discs and in some cases flash memory devices to various staff. These devices should only be used for business/college purposes (they should never be used for personal use) and are not an alternative to owning such devices for use outside of work. The named staff that are allocated this equipment are responsible for the appropriate use and safe storage of the equipment. Such equipment must be used in line with the rest of this strategy. College equipment must not be used in a way that violates Sense Data Protection Policy.

Please note that if college equipment is broken or damaged by use or misuse, it may only be replaced at the discretion of the College SMT and/or IT Team if possible within resource constraints. Equipment will not be replaced as a matter of routine outside of the normal cycle of replacement or upgrade.

College laptops may not be connected to the internet at another location, such as to a home network or hotel, without prior consultation with both the individual's line manager, College SMT or the IT Team. This will only be granted if the individual concerned can demonstrate a minimum level of competence and only then if they have a minimum specification of equipment at the remote end of the connection.

Part Nine: Use of Own Equipment / Mobile Technologies

Mobile computers and telephones belonging to an individual should only be used during breaks within the college unless there is a specific need for their use; this must be cleared with line management prior to such use. Mobile phones should remain switched off at all other times and should not be on the staff member's person unless the staff member has a clear business reason (as agreed by their line manager) to have the device with them or otherwise has permission from their line manager to use the device. Staff should never use their own telephones to contact learners/supported individuals and/or their parents/carers; if contact with learners/supported individuals and/or their families is required, a college telephone or college mobile should be used.

Under no circumstances should any personal audio visual equipment of any kind be used within college. Staff are prohibited from taking recordings or photographs of learners/supported individuals or learning activity within college or on trips outside of college when on college business, using their own personally owned equipment. This includes the use of camera phones and other similar devices.

If staff wish to have access to business/work related email or calendars on their personally owned mobile device they must justify a business case to the College SMT. A member of the College SMT will have the right of refusal to such requests. The device must be encrypted and locked with a passcode or other mechanism such as the Apple TouchID sensor. Additionally, staff members must agree to a remote wipe capability being enabled which allows the college to wipe the device remotely in the event of it being lost or stolen, in order to protect the data contained on the device. Any college connected device must have a screen lock enabled to prevent unauthorised access to the device.

Part Ten: Software

No college software should be copied under any circumstances. No software should be downloaded from the internet and either installed on college machines or burned onto CDs for use elsewhere.

All machines will have the appropriate basic software installed. Staff should not attempt to install or uninstall any software or otherwise change a computer's settings, other than those that relate to their individual profile such as accessibility options and preferences. If a member of staff feels they need access to software that is not currently installed, they should approach their line manager in the first instance. If deemed appropriate they will then approach the College SMT and/or IT Helpdesk to buy and install it. Software must not be installed by anyone except those authorised to do so. Software must never be taken from college to any non-college machine. This would constitute a violation of licensing agreements and is illegal.

Part Eleven: Copyright

The college respects and complies with copyright law. All users of the college systems must ensure that their use of the internet and materials taken from the internet complies with copyright law.

Users must not download or attempt to download copyright infringing material such as movies, games, music or software. Such activity is illegal. It is not acceptable for staff to store any music or other copyrighted files on the college computer system even if they own the original media such as a CD. Any staff found with 'copyright infringing' materials or attempting to use college equipment to infringe copyright will be subject to disciplinary action and their activities may be reported to the police for further investigation.

There are provisions in the CDPA (Copyright Designs and Patents Act) that permit teachers or learners to use and copy media for the purposes of instruction only. There terms are narrow and must be adhered to.

Running file sharing services such as bit torrent is strictly prohibited. Many of these services can install 'malware' onto the computer which they run on which can cause a range of problems from performance issues to providing a 'back door' for hackers to exploit. All of these services violate copyright laws and their use will not be tolerated.

Copyright infringement is a crime and this is currently being enforced by the government, police and the copyright holders, for which the penalties can be severe. The college can be audited by trading standards to detect any misuse and enforce the law without notice at any time.

Part Twelve: Data Protection / File Storage

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR) and Sense's policies and procedures.

Staff members of Sense College have access to confidential information about the college and/or our learners/supported individuals. It is not permissible to make any of this information available to others.

Any staff member intending to remove any data from a college site (be it in electronic or paper form) must gain explicit authority by an ESM or member of the College SMT on each occasion. This procedure also applies to all video created in the college. No video material may be removed from the college sites in any form without the explicit consent of a member of the College SMT. This permission must be obtained in every instance.

Any use of Sense data outside of the college (for example, in a piece of academic or professional development work) must be authorised by an ESM or member of the College SMT.

No data of any kind, including photographs should be made available outside of the college environment without appropriate permission being given, if in any doubt you should contact an ESM or member of the College SMT for advice.

Very sensitive data should only be stored on the college computer system in the appropriate place, with correct access controls. Data in this category includes personnel records, learner health and medical records and other confidential related materials and certain management data. It is the responsibility of line management to determine what data falls into these categories.

It is not acceptable for data of this nature to be stored on any removable media or devices, such as flash memory sticks, CDs, DVDs, portable hard discs and the like. If sensitive data has to be located on a removable device or media for business purposes, this should be encrypted in all cases. Only members of the College SMT or those specifically deputised by the leadership team should carry such media or devices.

Please note that even when given permission to remove data from a college site, it must be handled very carefully. It is the individual member of staff's responsibility to ensure the safety of the data. If any media or computer that is used to store data is lost or stolen, this must be reported immediately and investigated by line management.

College staff should understand that their college issue laptop or tablet may be checked from time to time to ensure compliance with this procedure. Video should never be loaded onto the network without the express knowledge and permission of either the College SMT or IT Team. There are storage limits in force on most areas of the network.

All college laptops that are issued to individuals will be encrypted. Loan machines should never be removed from the college sites/centres if they contain any sensitive data of any kind. Laptop encryption keys will be issued by the IT Team on an individual basis and will also be retained by the team. DO NOT disclose any encryption keys to any person outside of the IT Team. Please note that incorrectly entering an encryption key three times may result in the total destruction of all data on the computer. It may be irretrievable in this case. DO NOT record the encryption key in the same location as the laptop, such as on paper documents kept in the bag.

Any files stored on the services will be backed up with the daily routine. Files will be restored from the Sense backup if there has been a failure on the server. If files are accidentally deleted they may be restored at a time that is at the discretion of the IT team; as this is a time intensive process and can only be done at certain points in the server backup cycle.

Part Thirteen: External Access to College Networks

Access to the Sense College network from outside of the college sites is available to only those staff who need it as part of their role, apart from emails, the intranet and SMILE. Access to all services is via a secure web portal or available on a separate web address. Additional access to other resources is only available to selected management and technology staff via the Sense set VPN. Guidance on how to access these systems will be provided on request by the IT Team if College SMT authorises the staff member to have access.

Staff who access the college systems from the internet must use a computer that is:

- Fully patched with all the latest operating system security updates;
- Running up to date and approved security software such as firewall/anti-virus and anti-malware applications;
- Is using a modern operating system as advised by the IT Team.

Senior staff with elevated access should only use their college issued laptops for access to the college systems.

If any staff requires guidance around these requirements they should contact the IT Helpdesk in the first instance.

Part Fourteen: Roles and Responsibilities

It is the responsibility of all college staff to encourage learners/supported individuals to use computers and other technology appropriately and in a way that both promotes e-Safety and maintains this strategy. It is the explicit responsibility of teaching staff to ensure that any access to the internet is put to appropriate use within sessions and any users adhere to the e-Safety guidance (**Appendix 5**).

Learners/Supported Individuals

Learners/supported individuals will be expected to act safely and responsibly at all times when using the internet and/or mobile technologies.

Learners/supported individuals will need to discuss any concerns or worries with their personal tutor, key worker or a member of college staff.

Learners/supported individuals are responsible for using college equipment and network systems appropriately in accordance with this procedure.

Staff

All staff are responsible for using college IT systems and mobile devices in accordance with this strategy and Sense's OS26 Social Media Procedure, HR22 Social Media Policy and the ICT010 Social Media Safety Guidance.

All digital communications with learners/supported individuals must be professional at all times and staff members should be aware of the procedures surrounding their own use of social media both in and out of work as detailed in the Staff Handbook which is available via IRIS.

Staff should apply all relevant college procedures, policies and strategies and understand how to raise concerns and report incidents.

Staff should follow the safeguarding reporting procedures in line with the Sense OS11/OS12 Safeguarding procedures.

It is the responsibility of all staff to abide by this strategy and report any suspected or actual violations of it to their line manager.

Managers

Sense College managers and leaders will keep up to date with new technologies and their uses.

Managers and leaders will report and record all incidents appropriately and if required, raise safeguarding alerts.

Managers and leaders will obtain all relevant permissions and consents from individuals where appropriate.

It is the responsibility of the managers to ensure that violations or suspected violations of this strategy are elevated to the College SMT as soon as possible.

It is the responsibility of the College SMT to ensure that the college computer systems are operated legally and in order to meet statutory requirements such as the Prevent Duty.

Part Fifteen: Risk Assessment

Risk Assessment is about positive and informed risk taking and shouldn't focus on limiting or restricting people's access to technology.

When making use of new technologies and external online platforms, all staff and learners/supported individuals must assess the risk and if a significant risk can be identified, staff should complete a risk assessment.

Risk assessments of this nature should be conducted in accordance with Sense Health and Safety procedures with specific, dynamic and general risk assessments being put in place where necessary.

The college will risk assess emergent technologies and will also audit the use of existing technology to establish if this strategy and its implementation is adequate. An example

would be that the college will take reasonable steps to filter the internet connection and will continue to monitor this systems effectiveness.

Failure to follow the information stated in this strategy could lead to the following consequences:

- Unintended or unauthorised sharing of learners/supported individuals and/or staff personal data leading to loss of privacy or exposure to fraudulent activity;
- Sense College resources becoming exposed to harmful activity from internal and/or external sources;
- Reduction or loss of service from ICT network including network storage, workstations, internet, email intranet, etc;
- Loss of data;
- Additional costs to the organisation required to resolve any problems caused;
- Possibility of formal action as a result of not following this strategy;
- Possibility of criminal or civil legal action where an individual has failed to comply with this strategy and associated policies or legislation;
- Possibility of users (inclusive of learners/supported individuals and staff) being exposed to inappropriate materials (either accidently or purposefully) that may cause offence.

Part Sixteen: Communication

All staff and those learners/supported individuals who are issued with a user account must read this strategy and associated policies, procedures, strategies and guidance. Training and support can be provided. Users must also sign the relevant Acceptable Use Agreement.

Staff will be made aware of this strategy via a number of methods. Its importance will be communicated via email, college portal and staff meetings.

Learners and parents will be provided a copy of this strategy within induction packs and will be made aware of it during enrolment and/or review meetings, as appropriate.

Online communications can take many forms, whether it is by email, text, webcam or instant chat. It is essential that all staff and learners/supported individuals are aware of existing college strategies and processes that refer to acceptable behaviours when communicating online.

All users of Sense College IT systems (as well as all Sense staff) are expected to embody Sense's I-Statements at all times.

Any reported incident of bullying or harassment or other unacceptable conduct via technology, as noted within this e-Safety strategy, will be treated seriously and will be addressed through Sense College's Anti-Bullying Strategy.

With the unlimited nature of internet access in modern society, it is impossible for the college to eliminate all risks for staff and learners/supported individuals. It is our view therefore, that in addition to the Smoothwall monitoring system and Sense's policies/procedures, the college should support staff, learners/supported individuals and associates to stay e-safe through procedural guidance and targeted support to provide individuals with skills in order to identify risks independently and manage them effectively.

Learners/supported individuals should know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. In most cases this will be for the learners/supported individuals to indicate concerns to the most accessible member of staff at the time. Concerns can then subsequently be discussed further if need be.

Within sessions and activities, users will be encouraged to question the validity and reliability of materials researched, viewed or downloaded.

Part Seventeen: Handling Complaints and Breaches of Procedure

Any complaints that a member of staff has broken this strategy should be made to the individual's line manager who will elevate this via the line management system to an appropriate member of the College SMT.

Complaints or allegations that this strategy has been broken, such as misuse of the internet will be dealt with by a member of the College SMT. The e-Safety Strategy Flowchart (**Appendix 3**) will be used to process all complaints or breaches of this strategy, inclusive of complaints or concerns that relate to the Prevent Duty.

If there is any possibility that the breach is of a protection or safeguarding nature or any learner is suspected of coming to any form of harm, this should be elevated immediately to the Deputy Designated Safeguarding Lead and College SMT Designated Safeguarding Lead, who will activate the college's safeguarding procedure.

If there is suspicion of illegal activity this may be elevated to the police or other appropriate authorities at the discretion of the College SMT and Executive Principal.

Part Eighteen: Acceptable Use

Acceptable Use Agreements are intended to ensure that staff and learners/supported individuals will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use. In addition they ensure that college systems are protected from accidental or deliberate misuse that could put the security of the systems in jeopardy and also protect users from the potential of upset or harm when accessing digital technologies to enhance teaching, learning and work tasks.

In accordance with the information set out in this strategy, staff and learners/supported individuals that have user accounts and access Sense College's network, emails and internet (including via the Wi-Fi), must sign the appropriate Acceptable Use Agreement as per Appendix 1 and 2.

Part Nineteen: Third Party Account Access

Third party software is used within the college to perform certain management functions. The college's Management Information System (MIS) for the education provision, which links to the Individual Learner Record (ILR) reporting to the Education and Skills Funding

Agency (ESFA), is software provided by DatabridgeMIS. Although the data held is owned by Sense, the system is hosted externally and securely on DatabridgeMIS Ltd servers. A full contract and provider agreement is in place for this third party work and fully complies with GDPR compliance.

In the event of a third party (i.e. Smoothwall) needing access to the Sense system, a member of the College SMT authorises the work task and raises the request with the IT Helpdesk, who will work with the third party to provide access under observation, for the shortest time required only.

Part Twenty: Purposes of Safeguarding and Prevent Duty

The Prevent Duty is a specific set of responsibilities placed onto higher education, further education and skills providers (including Independent Specialist Colleges). The Counter-Terrorism and Security Act 2015 contains a duty on specified authorities to have due regard to the need to prevent people from being drawn into terrorism. The duty came into force on 18th September 2015 for further education. For other affected sectors, the Prevent Duty came in on 1st July 2015 (this includes schools and local authorities). The Prevent Duty does not apply in Northern Ireland.

Compliance with the Prevent Duty for publicly funded further education and skills providers in England is now monitored by Ofsted inspections.

The protection of learners/supported individuals and staff from the dangers of radicalisation and extremism is an aspect of safeguarding. Safeguarding is inspected as part of the effectiveness of leadership and management key judgement. It is recognised that Sense staff have a vital role in protecting the people we support from the risk of radicalisation. Keeping people safe from the risks posed by exploitation of social media and promotion through the internet by extremists should be approached in the same was as safeguarding people from any other online abuse.

Specifically, if you have a concern about the safety of a person at risk from radicalisation, you should follow the guidance set out in Sense College's Tackling Extremism and

Radicalisation Strategy. Local Authorities may also have a Prevent lead that can provide support, or the local police force can be contacted to talk to you in confidence about your concerns and help you gain access to support and advice.

Quality Assurance

The effectiveness of this strategy will be monitored and evaluated regularly, ensuring that there remains a clear, consistent focus on raising users e-Safety and positive engagement with stakeholders.

The monitoring process will include feedback from:

- Questionnaires and feedback;
- Annual Learner, Parent and Stakeholder Surveys;
- Compliments and/or Complaints;
- Feedback from Review Meetings and/or discussions;
- Management meetings and development review work;
- Leadership and Governing Body reviews.

The information and findings from these will be fed into the college self-assessment processes and support continued quality assurance and improvement.

This strategy and process will be reviewed:

- As the need arises;
- Following feedback on the documentation;
- Annually.

Conclusion

Sense College believes that an effective strategy of e-Safety can significantly enhance the quality of a learner/supported individual's journey and education provision by raising standards, increasing knowledge and confidence, ensuring safety within digital capabilities, as well as supporting staff to develop their practice.

For Quality Assurance Use only:

Policy/Procedure:	**Sense College E-Safety Strategy v05**
Author:	**Lynne Kendall, Head of Performance Management and College Improvement**
Quality Control:	**Lynne Kendall, Head of Performance Management and College Improvement & College Senior Management Team**
Date Live:	**August 2020**
Review Due:	**August 2021**