Chatsworth Futures
Specialist College

Online Safety Policy

Principles, processes and practice to secure learners' safety and well-being in relation to new technologies

Adopted: 15th September 2016

Last reviewed: 9th October 2021

To be reviewed: November 2022

Introduction

We live in a time when the protection of adults at risk is a significant concern within our society. Agencies have a moral and a statutory obligation to take every conceivable measure to safeguard the vulnerable adults they are responsible for.

At Chatsworth Futures, safeguarding adults at risk is a particularly pertinent and profoundly complex matter. Our learner population represents some of the most vulnerable members of our community and the manner in which we care for and protect the most vulnerable individuals in our society is the measure by which we should judge the quality of that society.

However, it is estimated that approximately 31% of people with disability experience some form of abuse during their lives. This is wholly unacceptable and it is the duty of all professionals and practitioners working with people with a disability to eradicate this disgraceful indictment of our society.

Alongside these generic safeguarding factors the young adults who attend our college are growing up at time in which the unprecedented growth in information and communication technologies presents both fantastic opportunities and significant risks. Consequently, any comprehensive and effective approach to safeguarding must take into account the specific vulnerability of our learners in this dynamic and rapidly expanding arena.

Chatsworth Futures is a specialist college within Salford Local Authority and as such is governed by the policies, procedures and practices of the Salford Adult Safeguarding Board. The following policy, written in line with guidance from the Salford Adult Safeguarding Board is based on Salford Local Authority's Online Safety Policy template. It is intended to support our college in developing a learning environment in which young people feel, and are, safe. This document reflects the important and complicated nature of safeguarding and each member of staff is required to have a secure working knowledge of the principles and practice described within this policy. At Chatsworth Futures the safeguarding of all our learners is everyone's responsibility.

Ethos

At Chatsworth Futures, we believe that all learners should be protected by those with responsibility for their well-being. We recognise that our learners are growing up in a world in which ICT will be a fundamental component of their experience of life and that we have a moral obligation to equip young people with the means to remain safe within that context.

Objectives

This Online Safety Policy is intended to consider all current and relevant issues in a whole college context and links to other policies related to learner well-being. This policy has been revised as our college becomes increasingly aware of the threat to our learners from on-line sexual grooming and online radicalisation. All members of our college community must remain vigilant at all times in order to protect our learners from these threats.

This Online Safety Policy applies to all members of the college community including staff, learners, volunteers, parents and carers, health professionals, social care colleagues, visitors, community users who have access to and are users of college ICT systems and mobile technologies, both in and out of college.

Practice

The practice described below is based on current best practice advice and will be consistently evident throughout our college community.

Roles and Responsibilities

The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the college.

<u>Governors</u>

- Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy

Principal

- The Principal is responsible for ensuring the safety (including Online Safety) of members of the college community
- The Principal should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff

The Chatsworth Futures Online Safety Co-ordinator is **Martin Hanbury**

Tutors and Teaching Assistants

- must have an up to date awareness of Online Safety matters and of the current college Online Safety policy and practices
- have read, understood and signed the college staff Acceptable Use Policy (AUP)
- ensure that they report any suspected misuse or problem to the Online Safety Co-ordinator

Designated Safeguarding Adults Lead is

- Martin Hanbury

The Safeguarding Team is

- Martin Hanbury
- Beth Cocken

of these **Martin Hanbury** has specific responsibility for Online Safety.

The person with responsibility for Online Safety should be trained in Online Safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal or inappropriate materials
- inappropriate on-line contact with others
- potential or actual incidents of grooming

- cyber-bullying

Learners

Whilst students within our college experience learning difficulties we can reasonably expect those students who access ICT independently to act with a measure of responsibility around their usage. Consequently students

- are responsible for using the college ICT systems and mobile technologies in accordance with the Learner Acceptable Use Policy
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

Parents

The college will take every opportunity to help parents understand any Online Safety issues. Parents and carers will be responsible for:

- endorsing (by signature) the student Acceptable Use Policy
- accessing the college ICT systems or Learning Platform in accordance with the Acceptable Use Policy.

Parents and carers can obtain support in the field of online safety through a number of different organisations. Below are two web addresses that are particularly helpful in protecting young people on-line

- https://protectyoung eyes.com/apps/
- https://swgfl.org.uk

Community Users

Community Users who access the college's ICT systems will be expected to sign a Community User Acceptable Use Policy (AUP) before being provided with access to our systems.

Online Safety Education and Training

Online safety education will be provided in a bespoke manner according to the age, cognitive ability and social understanding of each individual student. Online Safety may be addressed either through tutorial sessions or IT lessons as appropriate to the needs of learners.

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

Use of Communication Devices and Methods

The following table shows the college's policy on the use of communication devices and methods.

	Staff			**Other agencies, guests and visitors**			**Learners**			
Communication method or device	Allowed	Allowed at certain times	Not allowed	Allowed	Allowed at certain times	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to college	☑			☑					⚠	
Use of mobile phones in lessons			☒			☒				☒
Use of mobile phones in social time	☑					☒			⚠	
Taking photos on personal mobile phones or other camera devices			☒			☒				☒
Use of personal hand held devices eg PDAs, PSPs		⚠			⚠				⚠	
Use of personal email addresses in college, or on college network	☑				⚠					☒
Use of college email for personal emails			☒			☒				☒

Use of chat rooms / facilities			☒			☒			☒
Use of instant messaging		⚠			⚠				☒
Use of social networking sites			☒			☒			☒
Use of blogs			☒			☒			☒

Inappropriate Activities

At the heart of all practice at Chatsworth Futures is the safety and well-being of our learners. Any member of the college community who compromises this fundamental principle will be disciplined in line with Salford Local Authority's disciplinary procedures. Any member of the college community found to be acting illegally will be reported immediately to the police.

The college believes that the activities referred to in the following table would be inappropriate in a college context and that users, as defined below, should not engage in these activities.

User Actions	
The dissemination of any information which may be offensive to colleagues or breaches the integrity of the ethos of the college or brings the college into disrepute	☒
Using college systems to run a private business	☒
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SCC or the college	☒
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions	☒
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)	☒
Creating or propagating computer viruses or other harmful files	☒
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet	☒

On-line gaming (educational)	☒
On-line gaming (non educational)	☒
On-line gambling	☒
Use of social networking sites	☒
Use of video broadcasting e.g. Youtube	☒

Good practice guidelines

E-mail

Best practice

☑ **DO**

Staff and learners should only use their college email account to communicate with each other

Safe practice

Check the college Online Safety policy regarding use of your college email or the internet for personal use e.g. shopping

Poor practice

☒ **DO NOT**

Staff: don't use your personal email account to communicate with learners and their families.

Images, photos and videos

Best practice

☑ DO

Only use college equipment for taking pictures and videos.

Ensure parental permission is in place.

Safe practice

Check the Online Safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Principal's knowledge or permission

Make arrangements for pictures to be downloaded to the college network immediately after the event.

Delete images from the camera or device after downloading.

Poor practice

☒ **DO NOT**

Don’t download images from organisation equipment to your own equipment.

Don’t use your own equipment without Principal’s knowledge or permission and in accordance with the Online Safety policy.

Don’t retain, copy or distribute images for your personal use.

Internet

Best practice

☑ **DO**

Understand how to search safely online and how to report inappropriate content.

Safe practice

Staff and learners should be aware that monitoring software will log online activity.

Be aware that keystroke monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes will all be visible to the monitoring technicians

Poor practice

☒ DO NOT

Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings

Breach of the Online Safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.

Mobile phones

Best practice

☑ DO

If you need to use a mobile phone while on college business (trips etc), the college will provide equipment for you on request.

Safe practice

Check the Online Safety policy for any instances where using personal phones may be allowed.

Staff: Make sure you know how to employ safety measures like concealing your number by dialling 141 first.

Poor practice

☒ DO NOT

Staff: Don't use your own phone without the Principal's knowledge or permission.

Don't retain learner or parental contact details for your personal use.

Social networking

Best practice

☑ DO

If you have a personal account, regularly check all settings and make sure your security settings are not open access.

Ask family and friends not to post tagged images of you on their open access profiles.

Safe practice

Don't accept people you don't know as friends.

Be aware that belonging to a 'group' can allow access to your profile.

Poor practice

☒ DO NOT

Don't have an open access profile that includes inappropriate personal information and images, photos or videos.
Staff:

- Don't accept learners or their parents as friends on your personal profile.
- Don't accept ex-learners users as friends.
- Don't write inappropriate or indiscrete posts about colleagues, learners or their parents.

Webcams

Best practice

☑ DO

Make sure you know about inbuilt software facilities and switch off when not in use.

Safe practice

Check the Online Safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Principal's knowledge or permission

Make arrangements for pictures to be downloaded to the college network immediately after the event.

Delete images from the camera or device after downloading.

Poor practice

☒ DO NOT

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment without Principal's knowledge or permission – and in accordance with the Online Safety policy.

Don't retain, copy or distribute images for your personal use.

Disciplinary Processes

Any member of staff found to be in breach of this policy will be immediately subject to standard disciplinary processes. Where the breach constitutes an illegal act the police will be informed and due process will follow.

Any learner who knowingly breaches this policy will be subject to the procedures for sanctions depending on the severity of the breach, previous breaches of the college's codes of conduct and the likelihood of the offence being repeated.

Any other professional, guest or visitor found to be in breach of the policy will be removed from the site and refused access until further notice. Where the breach constitutes an illegal act the police will be informed and due process will follow.

Conclusion

In the modern era information technology has become interwoven into the fabric of our society and culture. Everything we do links with information technology. This includes our commitment to safeguarding and therefore the successful implementation of this policy is as vitally important as the implementation of all safeguarding measures.

This policy should be read in conjunction with all pertinent policies, guidance and documentation.

Appendix 1

Learner Acceptable Use Policy Agreement Template

This Acceptable Use Policy is intended to make sure:

- That you will be a responsible user and stay safe while using the internet and other technology for learning and personal use
- That ICT systems and users are protected from accidental or deliberate misuse

The college will try to ensure that you will have good access to ICT to enhance your learning and will, in return, expect you to agree to be a responsible user.

Please make sure you read and understand the following ☑ **I WILL** and ☒ **I WILL NOT** statements. If there's anything you're not sure of, ask your teacher.

☑ I WILL:

- treat my username and password like my toothbrush – I will not share it, or try to use any other person's username and password
- immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online
- respect others' work and property and will not access, copy, remove or change any one else's files, without their knowledge and permission
- be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- only use my personal handheld/external devices (mobile phones/USB devices etc) in college if I have permission
- understand that, if I do use my own devices in college, I will follow the rules set out in this agreement, in the same way as if I was using college equipment
- immediately report any damage or faults involving equipment or software, however this may have happened
- only use chat and social networking sites with permission and at the times that are allowed

☒ I WILL NOT:

- try (unless I have permission) to make downloads or uploads from the Internet
- take or share images (pictures and videos) of anyone without their permission
- use the college ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.
- try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes
- attempt to install programmes of any type on a machine, or store programmes on a computer
- try to alter computer settings

Learner Acceptable Use Agreement Form Template

This form relates to the Learner Acceptable Use Policy (AUP), to which it is attached.

I understand that I am responsible for my actions, both in and out of college:

- I understand that the college also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of college and where they involve my membership of the college community (examples would be cyber-bullying, use of images or personal information)

- I understand that if I fail to follow this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the college network/internet, detentions, exclusions, contact with parents and in the event of illegal activities involvement of the police

I have read and understand the above and agree to follow these guidelines when:

- I use the college ICT systems and equipment (both in and out of college)

- I use my own equipment in college (when allowed) eg mobile phones, PDAs, cameras etc

- I use my own equipment out of college in a way that is related to me being a member of this college e.g. communicating with other members of the college, accessing college email, Learning Platform, website etc

(Parents/carers are requested to sign the permission form below to show your support of the college in this important aspect of the college's work).

Name of Learner		
Group		
Signed (Learner)		Date
Signed (Parent/Carer)		Date

Appendix 3

Staff, Other Agency's Staff, Volunteer and Community User Acceptable Use Policy Agreement Template

College Policy

This Acceptable Use Policy (AUP) is intended to ensure:

- that staff, other agency's staff, volunteers and community users will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that college ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff, other agency's staff, volunteers and community users are protected from potential risk in their use of ICT in their everyday work.

The college will try to ensure that staff, other agency's staff, volunteers and community users will have good access to ICT to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff, other agency's staff, volunteers and community users to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use college ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students/learners receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online Safety in my work with young people.

For my professional and personal safety:

- I understand that the college will monitor my use of the ICT systems, email and other digital communications.

- I understand that the rules set out in this agreement also apply to use of college ICT systems (eg laptops, email, VLE etc) out of college.

- I understand that the college ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the college.

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will be professional in my communications and actions when using college ICT systems. I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the college's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the college website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in college in accordance with the college's policies.

- I will only communicate with students/learners and parents/carers using official college systems. Any such communication will be professional in tone and manner.

- I will not engage in any on-line activity either in or out of college that may compromise my professional responsibilities or damage the reputation of the college.

The college and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the college:

- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in college, I will follow the rules set out in this agreement, in the same way as if I was using college equipment. I will also follow any additional rules in line with the College's Online Safety Policy set by the college about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not use personal email addresses on the college ICT systems.

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

- I will ensure that my data is regularly backed up, in accordance with relevant college policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in college policies.

- I will not disable or cause any damage to college equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Local Authority Personal Data Policy. Where personal data is transferred outside the secure college network, it must be encrypted.

- I understand that data protection policy requires that any staff or student / learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by college policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for college sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Staff, Other Agency's Staff, Volunteer and Community User Acceptable Use Agreement Form

This form relates to the Acceptable Use Policy (AUP), to which it is attached.

I understand that I am responsible for my actions in and out of college:

- I understand that this Acceptable Use Policy applies not only to my work and use of college ICT equipment in college, but also applies to my use of college ICT systems and equipment out of college and my use of personal equipment in college or in situations related to my employment by the college.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police

    - **I have read and understood the college's Online Safety Policy**

I have read and understand the above and agree to use the college ICT systems (both in and out of college) and my own devices (in college and when carrying out communications related to the college) within these guidelines.

Name	
Position	
Signed	
Date	

Appendix 4

Use of Digital / Video Images

The use of digital/video images plays an important part in learning activities. Students/Learners and members of staff may be using digital or video cameras to record evidence of activities in lessons and out of college. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the college website and occasionally in the public media,

The college will comply with the Data Protection Act and request parents / carers permission before taking images of members of the college. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Parents are requested to sign the permission form below to allow the college to take and use images of their children.

Permission Form

Parent / Carers Name	
Learner Name	

As the parent / carer of the above student / learner, I agree to the college taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the college.

I agree that if I take digital or video images at, or of, college events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed	
Date	