CONQUEST CENTRE

Conquest Farm, Norton Fitzwarren
Taunton, Somerset. TA2 6PN
01823 433614
info@conquestcentre.org.uk

Conquest Centre

ICT / Internet Safety & Acceptable Use Policy

Policy Owner	Data & Communications Manager
Date of Original Issue	08.2021
Policy Last Reviewed	01.2026
Date of Next Review	01.2027
Version	V2

ICT INTERERNET SAFETY & ACCEPTABLE USE POLICY

Table of Contents

	Page
1. Policy Statement	3
2. Data Protection	3
3. Disclosure of Information	3
4. Online Safety	3
5. Student / Client safety on Conquest Centre's Internet System	4
6. Filters and Monitoring	4
7. Information System Security	4
8. Gaining Access to Conquest Centre's Internet	5
9. Staff Using Work Devices Outside of Conquest Centre	5
10. Electronic Communications	5
11. Email	6
12. Social Networking Services	6
13. Publishing Images and Work	6
14. Handling E-safety Complaints	7
15. Assessing Risks	7
Roles and Responsibilities	7
16. The Centre Manager	7
17. The Designated Safeguarding Lead	7
18. Conquest Centre ICT Lead	7
19. All Staff and Volunteers	8
20. Policy Review	8
Appendix A - Information and Guidance	9
Appendix B - Resources	11

ICT INTERERNET SAFETY & ACCEPTABLE USE POLICY

1. Policy Statement

This policy applies to all members of Conquest Centre, including staff, clients, carers, parents, volunteers, visitors and Centre users who have access to and are users of Conquest Centres Information and communications technology (ICT) system (both within the confines of Conquest Centre and outside).
The aims of this policy are to ensure that individual's may benefit from the opportunities offered by Conquest Centre's ICT resources in a safe and effective manner and to protect Conquest Centre's ICT infrastructure from misuse and attack.

Conquest Centre recognises the value of modern technology systems and welcomes their development. We continually strive to enhance their appropriate use in order to promote the attainment of our clients. This policy is of paramount importance as our students' access to technology is currently becoming universal and increasingly more mobile. The technologies encompassed by this policy include all computer and internet technologies and electronic communication devices such as mobile phones and tablets.

This policy should also be read in conjunction with our Safeguarding and Anti-bullying policies.

Any cases of a breach of the policy will be referred to the Centre Manager and Conquest Centre ICT Lead.

2. Data Protection

Conquest Centre supports the objectives of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 and other legislation relating to Data Processing, including the Human Rights Act 1998, Regulation of Investigatory Powers Act 2000 and the Freedom of Information Act 2000.
Conquest Centre has a statutory obligation to process personal data in accordance with the provisions of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

Every member of Conquest Centre has an obligation to ensure that the information they process (use) is collected, maintained and disclosed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 and the Conquest Centre Data Protection Policy.

3. Disclosure of Information

Any use or disclosure of information held within Conquest Centre, without there being a legitimate purpose or legal basis, will be classed as unauthorised and is a criminal offence under Section 55 of the Act Right of Access (Subject Access Requests)

4. Online Safety

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation and online bullying: technology often provides the platform that facilitates harm. An effective approach to online safety empowers parents and Conquest Centre to protect and educate the whole Conquest Centre community in their use of technology and establishes mechanisms to prevent, identify, intervene in and escalate any incident where appropriate and where any person is at risk.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, racist or radical and extremist views;
- Contact: being subjected to harmful online interaction with other users; e.g. commercial advertising as well as adults posing as children or young adults and;
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; e.g. making, sending and receiving explicit images, or online bullying.
- Commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

5. Student / Client safety on Conquest Centre's Internet System

Use of Conquest Centre ICT is forbidden unless authorised, including network access.

- Network and Internet use and access is considered a Conquest Centre resource and a privilege;
- Students are taught what internet use is acceptable and what is not and given clear objectives for Internet use;
- Internet access is planned to enrich and extend learning activities.
- Staff guide students in on-line activities that will support engagement and plan for the students' age, ability and maturity.

6. Filters and Monitoring

Conquest Centre will be doing all that they reasonably can to limit student's and client's exposure to the above risks from Conquest Centre's IT system. As part of this process, we will ensure Conquest Centre has appropriate filters and monitoring systems in place.

In relation to Conquest Centre's responsibility towards safeguarding and promoting the welfare of students and clients, we provide them with a safe environment in which to learn, we consider the age range and abilities of the students/clients, the number of students/clients, how often they access the IT system and the proportionality of costs versus risks.

Whilst filtering and monitoring is an important part of the online safety picture for Conquest Centre to consider, it is only one part. We also consider a whole Centre approach to online safety. This includes a clear policy on the use of mobile technology at Conquest Centre. Many students/clients have access to the internet via 3G and 4G.

Whilst it is essential that we ensure that appropriate filters and monitoring systems are in place, we will be careful that "over blocking" does not lead to unreasonable restrictions as to what students/clients can be taught with regard to online teaching and safeguarding.

Designated staff can review files and communications to ensure that the system is being used responsibly. They also have the right to access computer storage areas, accounts and removable media, including USB Flash Drives and CD-ROMs;

Designated members of staff can remotely view computer screens at any time, without them knowing, in order to ensure compliance and appropriate use;

7. Information System Security

Conquest Centre IT systems' capacity and security are reviewed regularly.

Virus protection is updated regularly and security strategies are discussed regularly.

8. Gaining Access to Conquest Centre's Internet
Conquest Centre maintains a current record of all system users (including staff, volunteers and students) who are granted internet access.

All Staff, volunteers and students/clients must read and accept this policy before using any resource.

9. Staff Using Work Devices Outside of Conquest Centre
All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Phones to have a six digit password.
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Keeping operating systems up to date – always install the latest updates.
- Work devices must be used solely for work activities.
- If staff have any concerns over the security of their device, they must seek advice from the Conquest Centre ICT Lead.

10. Electronic Communications
Whilst a lot can be gained from anyone using electronic communications, Conquest Centre requires the following guidance to be followed during or involving Conquest Centre activities:-
Always

- Accept that there is a duty of care to all children and vulnerable people.
- Use your Conquest Centre email address.
- Separate your personal and Conquest Centre social networking identities.
- Use electronic communications in an open and honest manner and conduct yourself as you would in face-to-face communications.
- Ensure your personal networking profile is set to private or friends only.
- Choose your profile picture with care.
- Ensure you have the required permissions when uploading photos and videos online.
- Report any concerns to the Conquest Centre Manager.

Never

- Accept electronic communications with anyone under the age of 13.
- Accept friend requests on your personal account from anyone over whom you hold a position of trust.
- Use your personal social network account to communicate with anyone over whom you hold a position of trust.
- Post derogatory or malicious comments or use inappropriate language.
- Engage in a one-on-one conversation via chat or instant messaging facilities with anyone over whom you hold a position of trust.
- Deliberately browse, download, or upload material that could be offensive or illegal.

- Give out details such as address, phone number or location unless they are separate professional contact details.

Note: Please be aware that people can search for you online in order to make direct contact, so as well as always considering what you are posting on your personal accounts, you may also wish to consider not using your full name (possibly a nickname) so finding you is more difficult.

11. Email
Electronic mail (email) provides a quick and effective means of communication. Staff/students/clients must be made aware that they will be held responsible for the content of any email message they transmit and that they should not contain messages using language or content that is unacceptable. It is also recognised that some people may try to use email to identify and contact staff/students/clients for unacceptable reasons.

The following points should be supported at all times:

- Steps should be taken to verify the identity of any organisation or individual seeking to establish regular email with Conquest Centre or its staff/students/clients.
- Information should never be given that might reveal a clients' identity or their current whereabouts.

12. Social Networking Services
Access to Social Networking services (for example Twitter, YouTube, Facebook, Instagram, Snapchat, etc.) are not blocked at Conquest Centre.

Staff, volunteers and students using such sites outside of Conquest Centre have a duty to use them responsibly. Any incident of slander, abuse or defamation perpetrated on a social networking site which impacts upon one of our staff / student / client / volunteers, shall be treated as Cyber-bullying.

Specifically, Conquest Centre recognises its responsibility to safeguard the welfare of all children, young people and adults at risk, by protecting them from all forms of abuse which can occur through the use of electronic communications. Furthermore, the use of the internet, electronic communications and social media is an intrinsic part of everyday life and can present challenges in terms of how it is used responsibly. Conquest Centre recognises that through misuse, all forms of electronic communications can be actually or potentially harmful to others.

Communication between all those that work, volunteer or visit Conquest Centre is to be expected but the use of electronic devices and commercially produced software needs to be used in a way that keeps everyone safe and shows respect to others. Communication devices include mobile phones, computers and any device that can connect to the internet or exchange information from one device to another. Electronic communication is that between clients / parents / carers / guardians etc and Conquest Centre staff, students and volunteers as well as Conquest Centre staff interacting between each other.

13. Publishing Images and Work (see Photography, Images and Videos Policy)
Photographs that include staff/students/clients will be selected carefully and will be appropriate for the context;

- No full names will be used when featured on news articles sent to press unless agreed with the individual before release;
- No photographs are published without permission from the client/parent/carer/guardian etc.
- Individuals at Conquest Centre and using Conquest Centre IT systems are subject to the provisions of the Copyright, Designs and Patents Act 1988;

14. Handling E-safety Complaints
Any complaint about IT misuse must be referred to the Conquest Centre ICT Lead;

Complaints of a safeguarding nature must be dealt with in accordance with Conquest Centre's safeguarding policy and should be recorded or reported to the Designated Safeguarding Lead.

15. Assessing Risks
Conquest Centre takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a Conquest Centre's computer. Conquest Centre can accept no liability for the material accessed, or any consequences of Internet access.

Roles and Responsibilities
16. The Centre Manager
The Centre Manager is responsible for ensuring that staff understand this policy, and that it is being implemented consistently.

17. The Designated Safeguarding Lead
The DSL takes lead responsibility for online safety at Conquest Centre, in particular:
- Supporting the Centre Manager in ensuring that staff understand this policy and that it is being implemented consistently.
- Working with the Centre Manager, and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the safeguarding & child protection policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the safeguarding & child protection policy.
- Liaising with other agencies and/or external services if necessary

18. Conquest Centre ICT Lead
The ICT lead takes responsibility for equipment and usage at Conquest Centre, in particular:
- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure clients are kept safe from potentially harmful and inappropriate content and contact online while at Conquest Centre, including terrorist and extremist material.
- Ensuring that Conquest Centre ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring Conquest Centres ICT systems.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

- Ensure there is a secure and regular backup of data wherever possible. Nevertheless, individuals are still primarily responsible for backing up their own data and work.

19. All Staff and Volunteers

All staff, including volunteers are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Working with the DSL to ensure that any online safety incidents are logged on MyConcern and dealt with appropriately in line with the safeguarding & child protection policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the safeguarding & child protection policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Only publish Conquest Centre related work on the Website/Internet in line with agreed Conquest Centre policy.

20. Policy Review

The Data and Communications Manager is responsible for monitoring and reviewing this policy. This policy will be reviewed annually. In addition, changes to legislation, national guidance, codes of practice or government advice may trigger interim reviews.

Appendix A

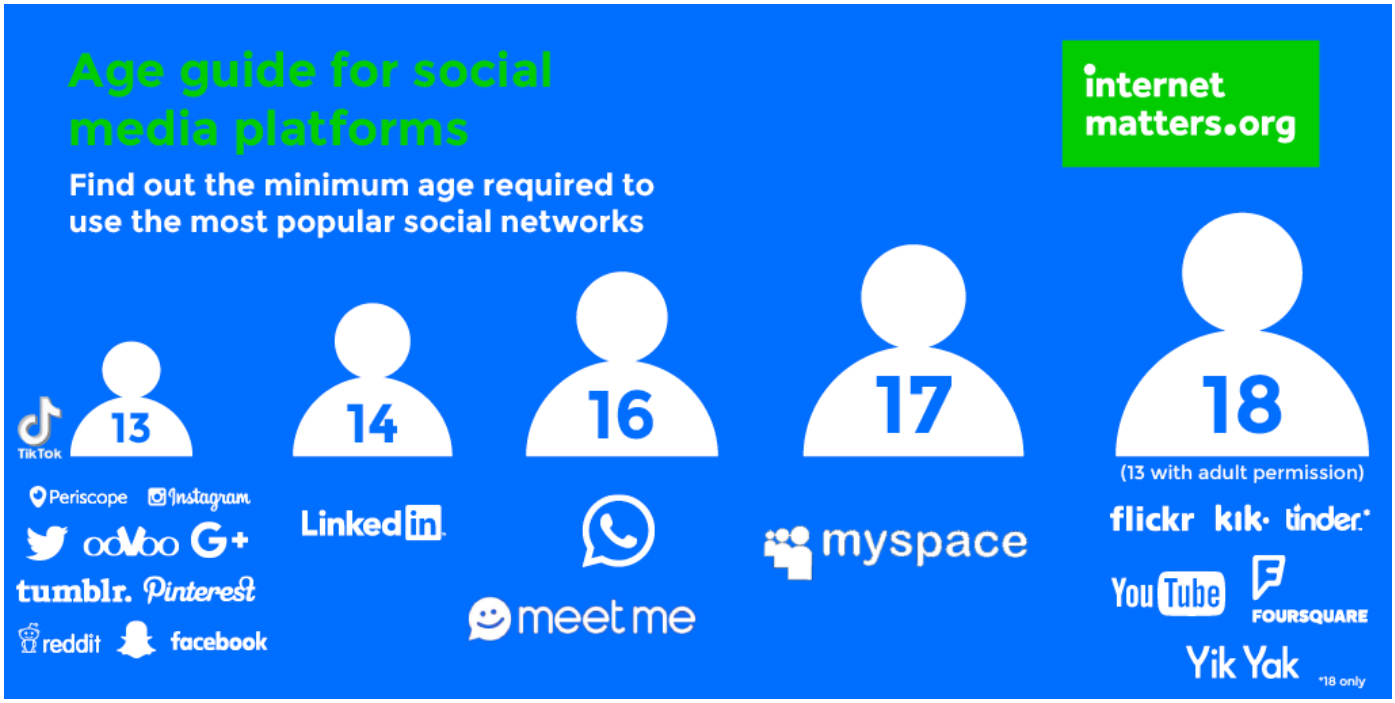
Information and Guidance

We offer all our staff a wide variety of IT resources which are under constant improvement and development. They are offered access to Conquest Centre's network, internet and electronic mail (email). Keeping our IT users 'safe' on the internet and supporting them to use the network appropriately is one of our key responsibilities. The Conquest Centre ICT / Internet Safety & Acceptable Use Policy will be explained to all new staff during their induction and then reiterated annually. Access to Conquest Centre's network, internet and electronic mail (email) will stop once an individual has left Conquest Centre.

It must be emphasised that the majority of our staff use the network, internet and electronic mail (email) safely and sensibly and this document acts to increase awareness for all. We take any infringement of the Policy very seriously and have installed software to monitor the use of the network, internet and email. Any case reported will be thoroughly investigated and judged on an individual basis.

It is Conquest Centre's policy that every reasonable step should be taken to prevent exposure of individuals to undesirable materials/contacts on the internet, including extremist propaganda or any site promoting radicalisation of any sort. It is recognised that this can happen not only through deliberate searching for such materials, but also unintentionally when a justifiable internet search yields unexpected results. To reduce such occurrences, Conquest Centre has its own dedicated broadband line and filter. This facility stops individuals accessing sites deemed inappropriate for use at Conquest Centre and also provides a full audit trail. We believe that the benefits to individuals from access to the internet exceed any disadvantages.

Please see the graphic below for the age restrictions for different social media platforms.



Here are the main e-safety issues, Conquest Centre staff/students/clients should be aware of:

- **Personal Identity Fraud:** there is a concern if students post personal details or complete online surveys. They should avoid giving out their full name, mailing address, telephone number, or any other information that could help someone determine their actual identity;

- **Public Domain Information:** all images, comments are stored and made available to the public. There are privacy settings and they should be used;

- **Online Bullying:** this can be in the form of comments, blog entries and chat rooms. Staff/students/clients must not send, share and upload of images, photos or videos that: - are illegal, obscene, and defamatory; - bring the school into disrepute or - are intended to annoy or intimidate another person.

- **Exploitation/ Misrepresentation:** clearly people may try to make contact with staff/students/clients and they may not be who they say they are. Staff/students/clients should never meet anyone they have met online.

Appendix B
Resources

CEOP
This is the web site of the Child Exploitation and Online Protection Centre (CEOP), which delivers a
multi-agency service dedicated to tackling the exploitation of children and young people. It provides advice to parents, carers and children and young people on Internet safety, an online reporting facility (Click CEOP) and the Thinkuknow web site (see below)

Thinkuknow
These resources help young people, parents and carers and teachers to learn about the risks that young people may encounter whilst using the Internet. Developed by the Child Exploitation and Online Protection Centre (CEOP) the Thinkuknow web site also includes a facility for young people to report online abuse.

Childnet International
This web site provides a range of resources to help children and young people to use the internet constructively and to protect children and young people from being exploited in the online environments provided by new technologies.

The **NSPCC's** online Net Aware(www.net-aware.org.uk) service provides expert reviews and safety advice on all of the most popular social networks, apps, and games young people are using.

Report Harmful Content online
Advice is provided on online issues such as bullying, harassment, threats,impersonation, unwanted sexual advances, violent content, suicide, self-harm and Pornographic content. https://reportharmfulcontent.com/

UK saferinternetcentre; where you can find e-safety tips,advice and resources to help children and young people stay safe online. For help and advice contact:03443814772 or helpline@saferinternet.org.uk

Revenge porn hotline; the only organization providing such a service in the UK, providing support and advice to the victims of the non-consensual sharing of intimate images and cyber-enabled blackmail (known as sextortion).

POSH
https://www.saferinternet.org.uk/helpline/professionals-online-safety- helpline
The Professionals Online Safety Helpline is a free service f or all professionals and volunteers working with children and young people. It provides signposting, advice and mediation to resolve online safety issues adults face about themselves, such as protecting professional identity and online harassment, or problems affecting children/young people, for example cyber-bullying or sexting issues. Where appropriate
we can also provide advice or facilitate in their removal on harmful content. POSH have created good relationships with many of the giant tech companies and are a great place to start if you have any concerns with a particular site or App.

Parentshield - The Child-Safe Mobile Network. https://parentshield.co.uk