CHISONA
ACADEMY
Embrace the Achiever in You

**CHISONA ACADEMY E-Safety and Online Access Policy. (Concise Version)**

Chisona Academy believes in the educational benefits of Digital Technologies for effective teaching and learning practices. Secure and effective internet access for pupils should be seen as an entitlement based on educational need and an essential resource for staff. We also recognize online safety issues and have developed plans that will help to ensure appropriate, effective and safe use by all. To help achieve this, we have implemented our online safety policy. Chisona Academy will commence her operations online.

## Policy Guidelines

This document has been designed to help monitor and manage our own online health and safety policy and is written with the following key principles in mind.

- All users are protected from inappropriate material, bullying and harassment.
- Users have access to resources to support learning and teaching.
- Users should be given clear boundaries on responsible and professional use.
- This policy also relates to our online FACT Sheets on E Safety, Child Protection and Safeguarding Policy, Online Health and Safety Policy, Staff ICT Policy, Equality and Behaviour policies that are all available on request or online at www.chisonaacademy.com

## Best Practice

Themes within this document are presented for discussion and adaptation so that it reflects best practice.  Chisona Academy is in regular consultation with all our stakeholders to constantly review the increasing threats across the internet.

## Disclaimer

Chisona Academy has made every effort to ensure that the information is accurate and up to date. If errors are brought to our attention, we will correct them as soon as is practically possible. However, Chisona Academy and employees cannot accept responsibility for any loss, damage or inconvenience caused as a result of any reliance on any content in this publication.

## 1. Leadership and Management

### 1.1 Developing a policy.

The provision online policy will feature as a part of the review process within the Provision Development Plan. It relates to other policies such as behaviour, anti-bullying, personal, social and health education (PSHE), child protection and Staff Code of Conduct and the prevent policy.

Our online policy has been written by the provision. It has been agreed by the Senior management and approved by the governing body and will be reviewed annually or in relation to new legislation or practice that needs immediate review.

### 1.2 Authorised Access

Internet access for pupils should be seen as an entitlement based on educational need and an essential resource for staff.

- All students are given an ICT Policy that is signed in accordance with the provision policy.
- All students, parents and tutors all have login accounts at www.chisonaacademy.com with secret passwords and email addresses as unique identifier.
- The provision will keep a record of all login access onto the website. The record will be kept up to date; for instance, if a student, parent, or tutor account is restricted or withdrawn.
- The provision expects that adult supervision is available for the students at all times during their online learning.

### 1.3 Filtering and Monitoring

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according to the pupils' age and experience. Internet access must be appropriate for all members of the provision community from the youngest pupil to the staff.

- A log of all staff with unfiltered access to the internet will be kept and regularly reviewed.
- A designated member of staff will review the popular permitted and banned sites access by the provision.
- The provision will work in partnership with parents, relevant authorities, DfE and cyber security to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the Internet Service Provider via the online safety lead.
- Websites logs will be regularly sampled and monitored by a nominee of the provision and reported to the Head of provision.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective, and reasonable.
- Any material(s) that the provision believes is illegal or may place an individual at risk must be referred to the appropriate authorities i.e., DSL, Health and Safety Manager, Head of provision, LADO, Police, Internet watch Foundation etc.

### Monitoring Extremism and Radicalisation

We also recognise the risk posed to our students of the online radicalisation, as terrorists organisations like ISIL see to radicalise young people through the use of social media and the internet. Research shows that ISIL propaganda included images and videos that present the group as an exciting alternative to life in the West and that it uses social media to encourage supporters to share the material with a wider online audience. The seriousness of the potential online threat is highlighted by the fact that 95, 000 pieces of terrorist content has been removed from the internet since 2010.

To combat this online threat, we recommend that responsible adults monitor the working of students online when students are logged in working from home or school. Chisona Academy staff will report any suspicious online behaviour to the academy manager. The Head of provision/Head of Safeguarding are notified on any inappropriate behaviour and appropriate steps are taken as required. This may involve speaking to the student, contacting parents, setting up a mentoring programme or making a direct referral to the MASH team based on the seriousness of the incident. Our annual staff training ensures all staff are fully aware of the risks posed by the online activity of extremist and terrorist groups.

E-Safety is a key aspect of the provision curriculum and equips pupils to stay safe online, both in provision and outside. E-Safety webinars will be delivered through the academy platform with specific focus on the risk that social media sites can pose to students.

For example;

- ISIL supporters use Facebook to share content, such as new stories and YouTube videos, among their peer groups.
- Twitter is a popular platform for pro-ISIL accounts. It is easy to establish an account, stay relatively anonymous and share materials.
- YouTube is used to host videos, both with official ISIL outputs and videos created by the users themselves. Multiple 'dummy' accounts will be set up so that when videos are taken down, they can be reposted quickly.
- ASK.FM is sometimes used by people considering travelling to Syria or Iraq and provides information on travel, living standards, recruitment fighting and broader ideologies.
- Instagram is used by fighters and ISIL supporters to share the photo sets frequently used by ISIL media organisations.
- Tumblr is an online blogging site and is used by ISIL fighters to promote longer, theological reasons as to why people should travel to Syria and Iraq. It is popular with female ISIL supporters, who have written blogs addressing the concerns girls have about travelling to the region, such as leaning their families and living standards in Syria.
- Private messaging apps, such as WhatsApp, Kik, SureSpot and Viber, are also commonly used to share messages on what to pack to travel and who to contact when they arrive.

E-Safety is also delivered in other subjects, such as PSHE, RSHE to complement our curriculum. All students also use the Education Training Foundation online safety and radicalisation resources to gain certification in their competency in these areas.

Chisona Academy is committed to providing a secure environment for pupils, where learners feel safe and are kept safe. All staff at Chisona Academy recognise that safeguarding is everyone's responsibility irrespective of the role they undertake or whether their role has direct contact or responsibility for learners or note. 'Safeguarding vulnerable people from radicalisations is no different from safeguarding them from other forms of harm' (Home Office, Prevent Strategy, June 2015).

In adhering to this policy, and the procedure therein, staff and visitors will contribute to Chisona Academy 's delivery of the outcomes to all learners, as set out in s10 (2) of the Children's Act 2004. Preventing Extremism and Radicalisation online is one element with our overall arrangements to safeguard and promote the welfare of all leaners in line with our statutory duties.

Our provision's Preventing Extremism and Radicalisation Online framework also draws upon the guidance contained in the DfE publication "Keeping Learners safe in Education, 2015", an specifically DCSF Resources "Learning Together to be Safe", "Prevent: Resources Guide", "Tackling Extremism in the UK", DfE's "Teaching Approaches that help build resilience to Extremism among Young People", Peter Clarke's Report (July 2014), "Keeping Children Safe in Education" (September, 2022), the "Counter-Terrorism and Security Act" (2015) and the "Prevent Duty" (June 2015).

### 1.4 Risk Assessment

As the quantity and breadth of the information available through the internet continue to grow it is not possible to guard against every undesirable situation. The provision will address the issues that it is difficult to remove completely the risk that pupils might access unsuitable materials via the provision systems.

- In common with other media such as magazines, books and video, some materials available via the internet is unsuitable for pupils. The provision will take all reasonable precautions to ensure that users access only appropriate materials. However, due to the international scale and linked nature of internet content, it is not possible to guarantee the unsuitable materials will never appear on a provision computer.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Head of provision will ensure that the internet policy is implemented and compliance with the policy monitored.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

## 2. Teaching and Learning

### 2.1 The Curriculum

The internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to be responsible, competent, confident and creative users of information and communication technology. In delivering the curriculum, teachers need to plan to integrate the use of communications technologies such as web-based resources, e-mail and mobile learning. Computer skills are vital to access life-long learning and employment; indeed, ICT is now seen as an essential life-skill.

- At the onset, all existing subjects will be delivered online at www.chisonaacademy.com
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The purpose of internet use in provision is to raise educational standards, to promote pupil achievement, ensure wellbeing, to support the professional work of staff and to enhance the provision's management information and business administration systems.
- Whilst internet access is an entitlement, users will need to show a responsible and mature approach to its use, or this privilege may be removed.

- The internet is an essential part of everyday life for education, business and social interactions. The provision has a duty to provide students with quality internet access as a part of their learning experience.
- Pupils use the internet widely outside provision and need to learn how to evaluate internet information and to take care of their own safety and security.

### 2.2 Enhancing Teaching and Learning

Benefits of using the internet in education include:

- Access to a variety of worldwide educational resources.
- Inclusion in the National Education Network which connects all UK provisions.
- Educational and cultural exchanges between pupils worldwide.
- Vocational, social and leisure used in libraries, clubs and at home.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments.
- Educational materials and effective curriculum practice.
- Collaboration across networks of provisions, support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Access to learning wherever and whenever convenient.

### 2.3 Evaluating Content

Information received via the web, email or text message requires good information handling and digital literacy skills. It may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

Ideally inappropriate material(s) would not be visible to pupils using the web, but this is not easy to achieve and cannot be guaranteed. Pupils should be taught what to do if they experience material(s) that they find distasteful, uncomfortable, or threatening.

- Pupils will be taught to be critically aware of the materials they read and how to validate information before accepting its accuracy.
- Pupils will age-appropriate tools to research internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-provision requirement across the curriculum.
- If staff or pupils discover unsuitable site(s) or content they consider to be inappropriate, the URL (web address) and content(s) should be reported to the nominated e-safety co-ordinator.
- Chisona Academy will ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to acknowledge the source of information used to add respect to the individuals and intellectual property when using internet material in their own work.

## 3. Communication and Content

### 3.1 Website Content

Publication of any information online will always be considered from a personal and provision security viewpoint. Sensitive information may be better published in the provision handbook or in our secure online area which requires authentication.

- Written permission from individuals, parents or carers will be obtained before photographs of pupils are published on the provision website.
- Pupils' full names will not be used anywhere on the website in association with photographs.
- The Head of provision will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Our website will comply with the provision's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

### 3.2 Learning Platforms

We will be implementing the Chisona Academy video conference classroom as our virtual learning environments (VLE) so that we can offer a wider range of benefits to teachers, pupils and parents, as well as support for management and administration. This is a bespoke platform enabling a first-degree security control and information access. Zoom platform with a subscription account could also be used as alternative substitute.

- All users will be required to use an age-appropriate password to access the relevant content of the LP which must not be shared with others.
- SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, parent/carer and staff community will have access to the LP.
- All users will be mindful of individual and intellectual property and will upload only appropriate content to the LP.
- When a user leaves the provision their account or rights to relevant content areas will be disabled.

### 3.3 Managing E-mail

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between provisions. However, the use of e-mail requires appropriate safety measures.

- Pupils may only use approved e-mail accounts on the provision system.
- Pupils must immediately tell a responsible adult if they receive offensive e-mail.
- Staff must use official provision provided e-mail accounts for all professional communications.
- Pupils should use e-email in an acceptable way. Sending images without consent, explicit images, messages that cause distress and harassment to others are considered significant breaches of provision policy and will be dealt with accordingly.
- E-mail sent to an external organisation should be written carefully and where appropriate, authorised before sending, in the same way as a letter written on provision headed paper.

**3.4 Online communications and Social Media.**

Online communications, social networking and social media services are filtered in provision by our content management system but are likely to be accessible from home.

All staff are made aware of the potential risks of using social networking sites or personal publishing either professional with students or personally. They are also made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material(s) may affect their professional status.

Pupils are encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image(s) or information once published. Chisona Academy plays a key role when teaching young people about the importance of how to communicate safely and respectfully online and keeping personal information private.

- Users will be taught about how to keep personal information safe when using online services. Examples would include real name, address, phone number, provision attended, IM and e-mail addresses, full names of family/friend, specific interest and clubs etc.
- Users must not reveal personal details of themselves or others in online communication, including the tagging of photos or videos, or to arrange to meet anyone.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and only operate with approval from the SLT or Governing Body.
- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the provision where possible.
- Pupils will be advised on security and privacy online and will be encourage to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invited known friends only on social networking sites and to deny access to others by making profiles private.
- No member of the provision community should publish specific and detailed and private thoughts about the provision and its community, especially those that may be considered threatening, hurtful or defamatory.
- Parents wishing to photograph or video at an event should be made aware of the provisions expectations and be required to comply with the provisions Responsible Use Policy (RUP) as a condition of permission to photograph and record.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of provision) will be raised with their parents/carers, particularly when concerning students underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the provision Responsible Use Policy.
- In line with 'Guidance for Safer Working Practice for Adults who Work with Children and Young People', it will not be considered appropriate for staff to engage in personal online communications with children and young people, parents and carers. Express care is also to be taken regarding the use of social networking sites.

### 3.5 Mobile Devices (including Bring Your Own Device – BYOD)

Mobile devices refers to any device that provides access to the internet or internal network(s) for example; tablet (Apple, Android, Windows and other operating systems), e-readers, mobile phones, ipads, ipod touch, digital cameras, smart watches.

Mobile devices can be used to facilitate communication in a variety of ways with text, images, sound and internet accesses all common features. A policy which prohibits users from taking mobile devices to provision could be unreasonable and unrealistic for provisions to achieve. Due to the widespread use of mobile devices, it is essential that provisions take steps to ensure that these devices, both personally and provision owned, are used responsibly.

Allowing the use of mobile devices is a provision decision, and should be subject to the following key principles:

- All individuals are protected from inappropriate material, bullying and harassment.
- Users have access to resources to support learning and teaching.
- Users should be given clear boundaries on responsible and professional use.

The following points, whist not exhaustive, have been provided to support provisions in creating effective policies.

- Mobile devices that are brought into the provision, remain the responsibility of the ser if not handed in at screening or late arrival. The provision accepts no responsibility for the loss, theft or damage of such items.
- Provision staff authorised by the Head of provision may search pupils or their possessions and confiscate any mobile device(s) they believe is being used to contravene provision policy, constitute a prohibited item, is considered harmful, or detrimental to provision discipline. If it is suspected that the material contained on the mobile device relates to a criminal offence, the device will be handed over to the Police for investigation.
- Sending abusive or inappropriate messages or content is forbidden by any user within the provision community.
- Mobile devices may not be used during lessons or formal provision time as a part of approved and directed curriculum-based activities unless authorised by the Head of provision or SLT.
- Mobile devices are not permitted to be used in certain areas or situations within the provision site e.g., changing rooms or toilets, situations of emotional distress etc.
- Where staff may need to contact children, young people and their families within or outside of the setting in a professional capacity, they should only do so via an approved provision account (e.g., email, phone, social media). In exceptional circumstances there may be a need to use their own personal devices and account; this should be notified to a senior member of staff ASAP.
- Staff will be provided with provision equipment for the taking of photos or videos of pupils linked to an educational intention. In exceptions circumstances staff may need to use personal devices for such a purpose and when doing so, should ensure that they comply with the provision’s policies.
- When in a physical space, for the safeguarding of all involved, users are encouraged to connect mobile devices through the provision’s wireless provision and service that allows the ability to filter any device that uses the provisions internet connection, without having to configure the user’s device.
- The provision will take steps to monitor responsible use in accordance with the ICT policy.

### 3.6 Video Conferencing

When in a physical space, video conferencing (including FaceTime, Skype, Good, Lync, Zoom and Teams) enables users to see and hear each other between different locations. This ‘real time’ interactive technology has many potential benefits in education and where possible should take place using the provision’s wireless system.

- All video conferencing equipment in the classroom must be switched off when not in use and all we cameras blocked.

### 3.7 Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, internet access, collaboration and multimedia tools. A risk assessment will be completed on each new technology and assessed for effective and safe practice in classroom use. The safest approach is to deny access until ta risk assessment has been completed and safety has been established.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in provision is allowed. E.g., CHATGPT AI Technologies

### 3.8 Cyber Bullying

Cyber bullying can be defined as “The use of Information Communication Technology (ICT) particularly mobile phones and the internet, to deliberately hurt or upset someone” DCSF, 2007.

For most, using the internet and mobile devices is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively.

It is essential that young people, provision staff, parents and carers understand how cyber bullying is different from other forms of bullying, how it can affect people and how to response and combat misuse. Promoting a culture of confident users will support innovation and safety.

Cyber bullying (along with other forms of bullying) of or by any member of the provision community will not be tolerated. Full details are set out in the provision’s behaviour, anti-bullying and child protection policies, which include;

- Clear procedures set out to investigate incidents or allegations of cyber bullying.
- Clear procedures in place to support anyone in the provision community affected by cyber bullying.
- All incidents of cyber bullying reported to the provision will be recorded.
- The provision will take steps to identify the bully, where possible and appropriate. This may include examining provision system logs, identifying and interviewing possible witnesses, and contacting the ISP and the police, if necessary.
- Pupils, staff, and parents/carers will be required to work with the provision to support the approach to cyber bullying and the provision’s e-safety ethos.

### 3.9 Data Protection

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen, or misused. The Data Protection Act, 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information and is referenced in our Data Protection Policy.

## 4. Implementation

### 4.1 Policy in Practice – Pupils

Many pupils are very familiar with internet use and the culture that surrounds it. As a part of the provision's e-safety teaching and awareness-raising, it is important to discuss the key features with pupils/students as appropriate for their age. Pupils may need to be reminded of the provision rules at the point of internet use.

- All users will be informed that network and internet use will be monitored.
- Online Safety teaching is integral to the curriculum and raises awareness and the importance of safe and responsible internet use amongst pupils.
- Online Safety teaching will be included in Princes Trust, PSHE, Citizenship and/or ICT and cover safe use at provision and home.
- Online Safety rules are in the ICT policy.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum and subject areas.

### 4.2 Policy in Practice – Staff

It is important that all staff feel confident about using new technologies in teaching and the Provision Online Safety policy will only be effective if all staff subscribe to its values and methods. Staff are given opportunities to discuss the issues and develop appropriate teaching strategies.

Consideration will be given when members of staff are provided with devices by the provision which may be accessed outside the provision network. They must be clear about the safe and appropriate use of provision equipment and follow the rules about eh use of equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of provision information.

If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their senior leader to avoid any possible misunderstanding.

- Staff should be aware that internet traffic is monitored (and automatically reported by the Security System) and can be traced to the individual user. Discretion and professional conduct are essential.
- Up-to-date and appropriate staff training in safe and responsible internet use, both professional and personal, will be provided for all members of staff.
- All members of staff will be made aware that their online conduct out of provision could have an impact on their role and reputation within provision. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

### 4.3 Policy in Practice – Parents

Parents need to be aware of the potential dangers that are associated with online communications, social networking sites and mobile technologies to help ensure their children are not putting themselves at risk.

Provisions may wish to refer parents to websites referred to in the reference section of this document.

- Parent’s attention will be drawn to the Online Safety Policy and the ICT policy via the Website and Latest News Alerts.
- A partnership approach with parents will be encouraged. This could include offering parents evenings, demonstrations, practical sessions and suggestions for resources and safer internet use at home.
- Internet issues will be handled sensitively to inform parents without undue alarm.

### 4.4 Handling of complaints

Parents and teachers must know how and where to report incidents in line with the provision complaints policy. Complaints of a child protection nature must be dealt with in accordance with the LA Child Protection procedures. Prompt action will be required if a complaint is made. The facts of the case will need to be established; for instance, whether the internet use was within or outside provision. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to the provision’s behaviour policy. All records of the incident should be kept e.g., emails saved or printed, text messages saved etc.

- Responsibility for handling incidents is managed by the Health and Safety Manager
- Any complaint about staff misuse must be referred to the Head of provision and logged on to the ICT portal by SLT.
- Pupils and parents will be informed of the complaint’s procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

## Useful Information for Parents and the Local Community

## KEEPING CHILDREN SAFE ONLINE

Children love using technology and are learning to navigate websites, online games and consoles, and touch screen technologies like iPads, tablets and smartphones from a younger and younger age.

These frequently asked questions will provide you with useful information and tips that you can put into place at home, to help keep your young children safe.

1) **Where do I start?**

*The best way to keep your family safe online, and to understand your child's internet use, is to use it together. Conversations and active engagement with your children are key. Be positive and embrace the technologies that young children enjoy – look for family activities and games. Take time to explore the games and services that your children use and look out for safety features that may be available. This will help you to be more confident.*

2) **How can I supervise my child?**

*Placing your laptop or computer in a busy part of the house, e.g., the living room or kitchen can be helpful. This can make it easier for you to monitor / get involved in their technology use. Remember the internet can be accessed from many portable devices, for example smartphones, smartwatches and tablets. Portable devices may allow you to ensure your children are using them where you can see them.*

3) **Are there tools to help?**

*There are parental controls and filters available, to help you set safer boundaries for your children, but you will usually be required to set them up. Your internet service provider will provide free filters to help block age-inappropriate content for children and on the UK Safer internet center website you can watch video tutorials that show you how to find and set these up. All mobile phone operators also provide parental control for free.*

4) **Where can I report an issue?**

*Reports can be made to websites through safety/help centers and moderation services. If you are suspicious about the behaviour of others online, reports can be made to CEOP and inappropriate media content, online and offline can be reported via SafetyNet http://www.safetynetkids.org.uk/personal-safety/staying-safe-online/*

*NSPCC* https://www.nspcc.org.uk/services-and-resources/research-and-resources/2016/what-should-i-do-helpline-repor-online-abuse/

Some other useful links –

www.childnet.com/parents-and-carers/need-help

www.ceop.police.uk

## KEEPING YOURSELF SAFE ONLINE

The internet provides lots of opportunities for chatting with friends, playing games and creating your own content. To help you get the most out of the internet, we've brought together the latest information on staying safe online. Here are a few tips to keep yourself safe online.

Top tips

1. Protect your online reputation: use the services provided to manage your digital footprints and 'think before your post.' Content posted online can last forever and could be accessed by anyone.

2. Know where to find help: understand how to report to service providers and use block and deleting tools. If something happens that upsets you online, it's never too late to tell someone.

3.  Don’t give in to pressure: if you lose your inhibitions, you’ve lost control; once you’ve pressed send you can’t take it back.

4.  Respect the law: use reliable services and know how to legally access the music, film, and TV you want.

## SOCIAL MEDIA CHECK LIST

- Do you know your friends?
- Who can find what you post?
- Be in control of what you share online.
- How does your profile appear?
- Teenager user updates.
- How do you use your friends lists?
- Do you know how to deactivate your account?

### Think about your future.

Popular websites and social media platforms make it easy to build a web of friends and acquaintances, and share your photos, whereabouts, contact information and interests.  But be thoughtful about what you post; don’t put your safety or your future at risk.

**Never forget:  the words and images you post on the internet may be available for years . . . forever** and your profile may be viewed by future employers and provision admissions officials, as well as identity thieves, spammers, and stalkers.

### Making your online profile work for you instead of against you

Recent media coverage has highlighted a new, fast-growing trend among corporate recruiters and provision admissions officials: more than just “Googling” candidates, many are now monitoring social networking sites too.  Recent studies have shown that 1 in 10 admissions officers check for candidates on social networking sites and 30 percent of the time, this leads to rejections. These numbers are likely to continue to climb in coming years.

**So, what’s the best course of action?  Use your online profiles to your advantage!**

Treat it like a free place to promote yourself personally and professionally while staying connected with your friends.  When applying to provisions or conducting a job search, this is particularly true.

Web pages containing risqué photos and provocative comments about drinking etc. can make applicants look immature and lacking professional judgement.