INTERNET AND SOCIAL MEDIA POLICY

STAFF

NLS policy states that staff members are allowed to use any social networking site as long as they follow these guidelines regarding the impact social networking has on NLS. Failure to comply with the above is an invasion of privacy and may infringe Confidentiality Policy. The guidelines include but are not limited to:

- Staff must not publicly mention any of the children from NLS on their online profiles
- Staff must avoid writing indirect suggestive comments about NSL on their social networking sites e.g. "I've had a bad day at work"
- Staff must not publish photos of the children on their online profiles
- Staff must not publish photos of other staff at NLS on their online profiles; and
- Staff must not publicly write anything about other staff members on their social networking sites
- Staff must not use their mobile phones to take photos or go on social networking sites whilst at NLS
- Staff must not mention any of the companies that NLS works with on their social networking site; and
- In order to maintain professional boundaries staff should not accept personal invitations to be friends from parents or carers or children that you look after or have looked after that use the club. Please refer to our Behaviour Management policy.

Staff members are advised to set their online profiles as private so that only friends are able to see their information. This can help to prevent any accidental breaches of this policy.

Please be aware that serious breach of the Social Networking policy could result in disciplinary action.

EMPLOYEE HAVING CONTACT WITH PARENTS AND CHILDREN

NLS respects the legal rights of employees with regard to the use of social networking and the internet. In general, what an employee does in their own time is their affair and NLS recognises that some staff may wish to publish private material on the internet including, but not limited to, social networking websites. Any activities, however, in or outside of work involving the internet are prohibited by this policy if they affect or could affect the reputation or service delivery interests, job performance (of the member of staff concerned or others) in a negative way in the reasonable opinion of the governors.

Employees may face disciplinary action if they harass, intimidate or demean other employees or stakeholders of NLS on a social networking site. Employees must make every effort to ensure that any remarks on a social media website are credible and accurate with a disclaimer that the views are those of the member of staff and not of the employer. It is likely that to share confidential or private information about NLS, its employee on a social media site or the internet will result in a disciplinary investigation.

Understand that is recommended do not accept friend requests or communications from learners or their family members past or present. If there is a pre-existing relationship this should be discussed with DSL – Luke or Scott who will need to consider how this is managed provide staff with clear guidance and record action taken.

NLS does have the right to monitor employees through social networking sites or the internet if there is cause for concern with regard to the activities of a member of staff or an investigation was taking place then NLS would consider accessing social media sites. This covers both private and professional use of social media.

Communication with learners, parents/carers and colleges should be professional and take place via official setting communication channels e.g work provided emails/numbers to protect both staff and learners.

RIGHTS AND RESPONSIBILITIES

When using social networking sites and the internet staff should ensure that this does not damage the reputation of NLS (or yourself) whether this is carried out during the working day time or privately. Staff are personally responsible for the content they publish on social media sites and the internet and must be mindful that this information will be in the public domain. Employees must have regard to the fact that they will be responsible for any commentary which is deemed to be a breach of copyright, defamatory, libellous or obscene.

Staff are aware that civil legal or disciplinary action can be taken against staff if they are found to have brought the profession or NLS into disrepute. Under no circumstances should any member of staff either at work or in any other place make deliberately download or possess or distribute material they know to be illegal for example child sexual abuse material.

KEEPING CHILDREN SAFE ONLINE WITHIN OUR SETTINGS

- Appropriate filters and monitoring systems are in place to protect learners form potentially harmful online material.
- Luke, Scott and Staff are aware of how and why technology is used within the setting by staff and children this includes types and number of devices if they are connected and if so how.
- NLS ensures that access to the settings network and infrastructure is secure such as use of passwords, screen locks, protected devices if removed from site.
- NLS ensures appropriate filtering and monitoring are in place and the setting has documented how decisions have been made; advice regarding appropriate filtering and monitoring is available from the UK safer internet centre.
- Access to the setting's devices is managed and monitored.
- Setting devices are kept securely and in line with data protection requirements.
- Physical safety of users has been considered e.g posture of children/staff when using devices.
- Personal data is managed securely online in accordance with the statutory requirements of the general Data Protection Regulations and Data Protection Legislation, this includes online learning journals or apps if used.

MANAGERS/STAFF RESPONSIBILITIES WITHIN THE SETTINGS TO KEEP CHILDREN SAFE WHEN USING TECHNOLOGY

- Ensure children appropriately supervised whenever they are using devices.
- Check apps, websites and tools prior to using them with children this includes checking the result of searchers.
- Use age appropriate apps, websites and online tools with children – there are details of useful websites that will provide links to appropriate content at the end of the policy.
- Luke, Scott and staff model save practise when using technology with children.
- Ensure data is shared online in accordance with the settings Data Protection responsibilities.

TRANSPARENCY

It is recognised that the line between professional and personal business can sometimes be blurred. It is important that individuals are thoughtful about the content and potential audiences for anything contributed to a social media site or the internet. It is vital that employees should be honest about their identity, and, where appropriate, be clear that any views shared are the employees as an individual and not necessarily the views of NLS.

The use of social media on behalf of the Club should only be used in a way that will add value to NLS and should be discussed with Luke and Scott, and accordingly all employees have a duty to present accurate information and ensure that pupils, other staff and parents are not misled.

Any member of staff contacted by the published media or radio or television about a post they have made on a social networking site should inform Luke or Scott immediately.

MONITORING

NEXT LEVEL SPORTS USE OF SOCIAL MEDIA

NLS recognises that social media has many positives but is also very aware of the potential risks associated with social media. The following considerations will be made:

- Only photos posted on social media are of an activity. If a child is in a photo they must be unidentifiable, ie arms and back of heads in shot. If a group photo is posted children must be unidentifiable
- Only one nominated member of staff will be responsible for upkeep of social media pages
- This person must adhere to our camera policy. The safe use and storage of photos must be in line with our policy at all times to ensure safeguarding is paramount
- NLS does have the right to monitor employees through social networking sites or the internet if there is cause for concern with regard to the activities of a member of staff or an investigation was taking place then NLS would consider accessing social media sites. This covers both private and professional use of social media
- Photo's are to be deleted from cameras and Sim cards once they have been printed off/uploaded

LEGAL ISSUES

All employees of NLS should take the following into consideration when using social media:

- Be aware of the policy and guidelines for using social media whether this is for personal use or as part of the working role.
- Be familiar with the legal areas outlined below before writing about colleagues or sharing information about NLS.
- Ensure that posted material does not disclose privileged or confidential information.
- Remember that defamation is the act of making a statement about a person (or an institution) that is considered to harm their reputation. Where such a defamatory statement is written down (either in print or online) this is referred to as libel.

Action can also be taken against anyone repeating libellous information from another source so careful checks are needed before quoting statements from other social network sites or the internet.

EMPLOYEE HAVING CONTACT WITH PARENTS AND CHILDREN

NLS respects the legal rights of employees with regard to the use of social networking and the internet. In general what an employee does in their own time is their affair and NLS recognises that some staff may wish to publish private material on the internet including, but not limited to, social networking websites. Any activities, however, in or outside of work involving the internet are prohibited by this policy if they affect or could affect the reputation or service delivery interests, job performance (of the member of staff concerned or others) in a negative way in the reasonable opinion of the governors.

Employees may face disciplinary action if they harass, intimidate or demean other employees or stakeholders in the club on a social networking site. Employees must make every effort to ensure that any remarks on a social media website are credible and accurate with a disclaimer that the views are those of the member of staff and not of the employer. It is likely that to share confidential or private information about NLS, its employee on a social media site or the internet will result in a disciplinary investigation.

ONLINE SAFETY

This policy focuses on what we can do as individuals, parents, early years staff, professionals and others that educate ourselves and our children and young people to stay safe online.

Learning about staying safe online is a vital life skill. Knowing about risk and behaviour are the two fundamental principles of online safety because if you don't know about online risk, your own behaviour can put you at risk. Educating ourselves first gives us the knowledge to empower children and young people with the know-how to safeguard themselves and their personal information. Teaching children how to stay safe online is something that should be nurtured throughout a child's early and middle years, right through adolescence to see them into adult life.

THE POLICY COVERS

The four C's | What we can do as professionals and advice to parents | What we should teach children and young people | Reporting concerns | They say there are four Cs for potential risks facing children:

1. Content
Being exposed to harmful material.

2. Contact
Engaging with people who may not be who they say they are and/or may have ill intent. These may, occasionally, be sexual predators, attempting to groom children, potentially with the aim of meeting them offline. They may also be people who intend to threaten, intimidate or bully.

3. Conduct
The child or young person is the one displaying the inappropriate sexual or bullying behaviour or the victim of someone else's behaviour.

4. Commercialism
Being exposed to inappropriate commercial advertising, marketing schemes or hidden costs. These four Cs come into play at different stages of a child's development and so vulnerability is not a static issue but one that needs to be understood in the broader context of children's lives and their stage of emotional, psychological and physical development.

At NLS we are pro-active in ensuring that parents and staff know how to stay safe on line:
- Get involved
- What devices/apps are they using. Do they allow online interaction?
- Be aware of what young people are doing online
- Be 'friends' with your children on Facebook and other social networking sites
- Talk to them and ask what they are doing
- Use the parental controls on the operating systems
- Speak to your internet service provider about how you can filter internet access

EDUCATING USERS TO STAY SAFE ONLINE

- Set privacy settings and guard your information: Address; phone numbers; school; city or town, parent's workplace, passwords
- Guard your information: Technology can share information without knowledge; for example, turn off synchronisation on Android devices, turn off location services and switch on when required.
- Limit time online: Log off and play; take time for family and proper face-to-face time with friends.
- Friend or foe? Never schedule offline meetings with 'online only' friends; tell parents if anyone tries to meet you offline; not everyone is who they say they are.
- Communicate: Talk about it if someone has upset you; stay away from 'adult only' sections of the internet; tell your parents about anything that makes you uncomfortable; do not believe everything you see - just because it is on the internet doesn't mean it is true.
- Safety with webcams: Never do random chat (sites like Chatroulette); only chat with family and friends; never do anything on the webcam you wouldn't want up on the screen; think before uploading video responses.
- Time and place: Carefully consider whether to use geolocation (showing people exactly where you are) on social networks or games. Ask parents' permission before using it; do not use the internet for personal purposes at school or any place you visit regularly; check your privacy settings.
- Be 'scam smart': Don't open strange emails; beware of 'free' downloads that could hide viruses or spyware.
- Don't be a 'pirate' (e.g. access music, videos or films illegally); don't use peer-to-peer file sharing as it leaves you open to viruses, spyware and identity theft.
- Teamwork: Help your parents to protect you; help each other; communicate; cooperate; know when to log off.
- Safety sessions regularly form part of the programme of delivery to users.
- NLS make use of National and locally Local safeguarding Children Board (LSCB) approved resources

On online bullying specifically, what should we teach our children?

- Don't respond
- Don't retaliate
- Talk to a trusted adult
- Save the evidence
- Block the bully
- Be polite
- Don't be a bully
- Be a friend not a bystander

What should adults do?

- Listen and take the child seriously
- Make sure the child is safe and feels safe
- Don't overreact
- Encourage the child not to retaliate
- Gather the facts and save the evidence

TRAINING

- Staff are trained to follow best practice when using online technologies
- There is a planned programme of online safety training for all staff with induction and regular updates that support safeguarding practice
- The views of users are sought in the design of training programmes
- The training needs of staff are identified
- The availability of internal and external training is advertised to staff

REPORTING

All staff and users are aware of how to report concerns. The Designated safeguarding person is responsible for ensuring that:

- There are clear and understood systems for reporting safety incidents relating to service users and staff. Please follow safeguarding procedure
- There are clear escalation processes for the handling of incidents. Please follow Next Levels Sports safeguarding procedure
- Reporting systems are known by the whole organisation
- The culture of the organisation encourages all staff users and its wider community to be vigilant in reporting issues
- Issues raised will be dealt with quickly and sensitively
- Reports of incidents are logged and regularly audited and monitored
- The organisation actively seeks support from the local authority
- There are good links with outside agencies e.g police

REFERENCES FOR ADDITIONAL INFORMATION AND SUPPORT

- Childnet: For a range of educational materials and resources for use with children, parents and teachers, including 'Social networking: a guide for teachers and professionals' and 'Keeping young children safe online'
- DfE Data Protection Toolkit for Schools: For information on what schools need to do in order to comply with data protection regulations
- Information Commissioners Office (ICO): For information around data protection and GDPR
- Internet Matters: For a range of materials for parents and teachers, including for pre-school and 0-5
- NCA-CEOP: Education resources for use with children, parents and professionals and advice on safeguarding children from sexual abuse, including www.thinkuknow.co.uk and the CEOP Safety Centre

- NSPCC online safety
- Parent Zone: For a range of education materials and resources for use with children, parents and teachers
- Parent Info
- UK Safer Internet Centre: For a range of education materials and resources for use with children, parents and teachers, UK SIC helpline for professionals who are working with children and young people

ACCEPTABLE USE AND POLICY TEMPLATES

- www.kelsi.org.uk/child-protection-and-safeguarding/e-safety
- www.swgfl.org.uk/products-services/online-safety/resources/online-safety-policy-templates/
- safepolicies.lgfl.net

NLS LINKED POLICIES

- Child protection.
- Staff code of conduct.
- Use of Camera.
- Whistle blowing.
- Health and safety.
- Achieving positive behaviour.
- Anti-Bulling.
- Peer on Peer.
- Mobile phone.