Policy Focus	**E-Safety and Social Media Policy**
Lead Policy Holder	**Pete Jenkins (Executive Principal)**
Designated Director	**Judith Johnson**
Policy Date	**March 2019**
Policy Version	**Version: 2**
BoD Adoption	**November 2019**
Review Date	**July 2022**

School Aim

Our Company (Life Chance Education Ltd) is committed to transforming the life chances of the young people and families that we work with. We support children who have suffered trauma, Adverse Childhood Experiences (ACEs), and exhibit Social, Emotional and Mental Health difficulties (SEMH). Our educational staff, multi-disciplinary team of therapists, and support team work together to create an environment that meets the holistic needs of children who have difficult or complex life stories.

By delivering the best features of a special school and alternative provision, coupled to innovative educational and therapeutic frameworks, we can help our students thrive. We believe that children don't have to be bound by the past but can build a bright future if they have the right support.

Our Mission is to ensure that we help every child we work with achieve their full potential, both academically and personally. As a school we aspire to being outstanding, so our students can be too – as exemplified in our school motto:

'Being the Best We Can Be'

Our Aims are to:

- Meet the previously unmet needs of young people and enable learning and employment.
- Provide positive interventions into barriers to learning and negative family or intergenerational life cycles.
- Contribute to community and social change.
- Reduce costs to society in terms of both social and economic benefits

To reach these aims we will use concepts and best practice in learning, neuroscience, emotional well-being, child development and coaching.

Contents

1. Glossary of Acronyms
2. Statement of Intent for this Policy
3. Statutory / Legislative Basis
4. Links to Other Related Policies
5. Monitoring Review & Evaluation: Compliance - Consistency - Impact
6. Key Policy Information / Guidance Relating to our Practice
7. Implications for Stakeholders
8. Relevant Data Sets / Metrics
9. Relevant Resources
10. Appendices (Embedded / E.Links)

(Statutory Documents – Data Sets – Recording Templates – Resources - SoL etc)

Glossary of Acronyms

GDPR	General Data Protection Regulation
HoS	Head of School
ICT	Information and Communications Technology

1. Statement of Intent for this Policy

This Policy is to provide all staff with the necessary information to enable them to meet their responsibilities and to ensure consistent and effective practice across all school sites. It demonstrates the school's commitment with regard to the safe and responsible use of the internet, technology and social media to students, parents and other partners.

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Statutory / Legislative Basis

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association.

3. Links to Other Related Policies / Procedures

This policy sits within the Safeguarding Portfolio of Policies which School for Inspiring Talents has adopted. It therefore relates to other policies in that themed grouping which include:

- Anti-Bullying Policy
- Child Protection & Safeguarding Policy
- Contractors and Visitors Policy
- First Aid Policy
- Intimate Care Policy
- Lockdown Procedures
- Preventing Extremism & Radicalisation Policy
- Single Central Record

In addition, it links to our Code of Conduct which sits in the Personnel Portfolio.

4. Monitoring, Review & Evaluation (MRE): Compliance - Consistency – Impact

Monitoring, Review and Evaluation (MRE) of all aspects of our work as a school is undertaken to ensure that we are delivering on what we say we want to achieve with and for our students. In the interests of equity and high expectations for all our students, we are continuously checking for:

- Compliance and for Quality
- Implementation match with our Intent
- Consistency between staff and sites
- And to ensure value for money for our Referring Local Authorities.

Our school staff are part of our school culture of continuous improvement based on supervision, self-reflection, peer working, and CPD. Daily staff briefings and debriefings provide immediate feedback and strategies for even greater success next time round.

Our framework for MRE is achieved via 3 key approaches:

Internally

- Our annual Self Evaluation Position Statement (SEPS) aligned with Ofsted Evaluation Areas and Grade Descriptors
- Learning Walks by HoS in own and other Phases/Sites
- Individual Student Assessment Framework and Trackers
- CEO & Executive Principal's Observations, Spot Sampling and Random Checks
- Monthly SLT Progress Reviews of the Operational School Improvement Plan (OSIP)
- Heads of School Monitoring
- Appraisal & Performance Management approaches.
- SchoolPod, Incident Logs Reviews and Spot Sampling, plus trend monitoring across the year
- Staff Briefings
- Student Voice Surveys
- Peer Reviews through Team Working
- CPD Evaluations

Accountability MRE

- Our Board of Directors Link Portfolio Visits and Observations
- Director Monitoring of all Independent School Standards (ISS) Themes annually as part of a rolling programme
- Termly Directors Scrutiny of the CEO & Executive Principal Reports to the Board
- Termly H&S checks
- Directors Involvement in the cycle of Policy Review
- Financial and Curriculum Resource Monitoring

Externally

- Referring LAs' Annual Health Checks and Audits
- Commissioned Reviews of aspects of practice – specialist and generic e.g., Behaviour, Health & Safety
- Feedback from submissions for Awards and Quality Standards e.g., TISS
- Parent / Carer Feedback e.g.: via Class Dojo
- Ofsted Monitoring and Inspection Visits
- User Schools Feedback

5. Key Policy Content - Information / Guidance Relating to our Practice

Educating pupils about online safety
Pupils will be taught about online safety as part of the curriculum.
In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity

How to report a range of concerns

- The safe use of social media and the internet will also be covered in other subjects where relevant.
- The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.
- The Head of School, Family Practitioner or keyworker notifies parents of specific, relevant issues in a timely fashion.

Educating parents about online safety

- The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents
- Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of School and/or the DSL.
Concerns or queries about this policy can be raised with any member of staff or the Head of School.

Cyber Bullying
Definition

- Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).
- The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.
When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police
-

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.
Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.
On the guest network, access is only allowed after agreeing the above.

Pupils using mobile devices in school

Pupils may bring mobile devices into school but are handed into staff at the start of the day.
Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).
Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.
Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.
Any USB devices containing data relating to the school must be encrypted. If staff require one they should obtain it through the ICT manager.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.
Work devices must be used solely for work activities.

How the school will respond to issues of misuse
Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training
All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins, and staff meetings).
The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our child protection and safeguarding policy.

Social Media
SfIT recognises that many staff, directors, parents, carers, and pupils have a personal use for the internet and that they may participate in social networking on social media websites such as Facebook, Twitter, Instagram, etc.
Whilst staff, directors, parents and carers are free to use the internet in this way, they must ensure that they do not breach the law or disclose SfIT's confidential information, breach copyright, defame the school, its staff, directors, parents, carers and pupils. They must not disclose personal data or information about any individual that could breach the Data Protection Act 2018 (GDPR) or SfIT's E-Safety policy. They should keep completely confidential, any information regarding the children, their families or other staff which is learned through the school.

The purpose of this policy is to outline the responsibilities of staff, directors, parents, and carers who are engaging in social media, networking websites, blogs and using online dating websites.

Personal websites and blogs
The following guidelines apply:
- Staff, directors, parents, and carers must not disclose any information that is confidential to the school or any third party that has disclosed information to the school.
- Staff, directors, parents, and carers should not link any personal websites, social networking sites etc to the school's website.
- If a member of staff, directors, parent, or carer is asked to contribute to an official weblog connected to the school, then special rules will apply, and they will be told in detail how to operate and what to write.
- SfIT will not tolerate criticisms through social media. If a member of staff feels aggrieved, then they must follow the procedures outlined in the Complaints and Whistleblowing Policy.

Social networking sites
The school respects a member of staff's right to a private life. However, the school must also ensure that confidentiality and its reputation are protected.

The school expects all staff, directors, parents, and carers to:
- Ensure that they do not conduct themselves in a way that is detrimental to the school.
- Take care not to allow their interaction on these websites to damage working relationships between members of staff and clients of the school.

Important considerations
Staff, directors, parents, and carers should be aware that social networking websites are a public forum, particularly if they are part of a 'network'. Staff, directors, parents, and carers should not assume that their entries on any website will remain private.

When using social media, networking and online dating websites, staff, directors, parents, and carers should follow these guidelines:

- Staff should not accept friend requests from SfIT pupils, parents, or carers under any circumstances. Where relationships are already established, staff should proceed with caution, being fully aware of the social media guidelines and the teacher's code of conduct.
- Staff should increase their privacy settings whenever available.
- Staff should not share personal conversations.
- Staff should behave respectfully and should not engage in topics that may be considered objectionable or inflammatory such as politics or religion.
- Do not defame (libel) anyone. A member of staff, director, parent, or carer who makes a defamatory statement that is published on the internet may be legally liable for any damage to the reputation of the individual concerned.
- Do not post material that is abusive, defamatory, sexist, racist or that could be interpreted as harassment or bullying.

Personal use of the internet
SfIT does not allow personal use of the internet during work hours on school devices. All personal devices should be stored safely in the staffroom and only accessed during a recognised break.

Disciplinary action
If necessary, action will be taken against any member of staff, directors, parent, or carer who is found to have breached this Policy. Staff should also refer to the Disciplinary Policy.

Security and identity theft
Staff, directors, parents and carers must be security conscious and should stay proactive, taking steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and, for example, favourite football team which can form the basis of security questions and passwords.

Staff & Mobile Phones

- During their working school day staff mobile phones should only be used when in a staff only area.
- Mobile phones should be switched off and stored in a safe place not accessible by staff or children especially during lesson times. The school will not take responsibility for any items that are lost or stolen.
- Where a phone call is expected upon the mobile phone, staff are advised to leave it with staff in the admin office. They will be informed if the call is received. Staff are advised to give the school telephone number to be contacted upon during the school day.
- School excursions /residentials – staff are required to take a mobile phone to ensure they have full contact with school in case of an emergency. In such cases staff are expected to carry the phone upon themselves and if appropriate ensure it is not on silent. Staff are reminded of policy to not use for any other reason other than in communication with school or in an emergency.
- Strictly no photos should be taken of the children or activities. A school camera should be used for any photos.
- Staff should never contact students or parents from their personal mobile phone or give them their mobile number to students or parents. If a member of staff needs to make telephone contact with a parent or student, a school telephone should be used.
- With regard to camera mobile phones, a member of staff should never use their phone to photograph a student(s) or allow themselves to be photographed by a student(s).

This guidance should be seen as a safeguard for members of staff. Staff should understand that failure to comply with this policy is likely to result in the enforcement of our whistleblowing policy and associated procedures.

Staff work mobiles

The use of a designated work mobile is allowed as:

- An essential part of the emergency toolkit which is taken on off-site trips.
- A communication aid, enabling text, email messages and calls to be made and received from parents/carers and other professionals.
- A back-up facility should problems be experienced with the landline – or where contact needs to be made outside of work hours.
- As a safety measure for staff with an outreach function in their job role.

Staff who are permitted to use a work mobile phone should try not to use them in the presence of students and make sure they can't be over-heard when making confidential calls.

6. Implications for Stakeholders

Board of Directors	Provide access of this policy to all staff, visitors, parents/carers.
All Staff	It is the responsibility of all staff to follow the agreed ways of working as outlined in this policy. All staff should apply this policy on a daily basis, personalising and individualising its implementation to meet the specific needs of our pupils.
Designated Specialist Staff	The Online Safety Coordinator will monitor the application of this policy by other staff.
Students	Students will understand their responsibilities with regards to e-safety and social media use.
Families/Carers	Families/Carers will understand that whilst using the internet for personal use, they must ensure not to breach the law, disclose SfIT's confidential information, breach copyright, defame the school (staff, directors, parents/carers and pupils).

7. Relevant Data Sets / Metrics

N/A

8. Relevant Resources

NEU - Social Media and Online Safety
UK Safer Internet Centre - Social Media Checklist

9. Appendices

ICT Code of Conduct	Acceptable use agreement (pupils and parents/carers	Acceptable use agreement (staff, governors, volunteers and visitors)	Online safety training needs (self-audit for staff)	Online safety incident report log
ICT Code of conduct.docx	Acceptable use agreement (pupils	Acceptable use agreement (staff,	Online safety training needs –	Online safety incident report