



**EARLY LIFE**

ENTERPRISE | ENGAGE | INSPIRE

## **Social Media Policy**

Last Review on: June 2024

Next review due by: June 2025



## 1. Policy Statement

To ensure clarity of use and guidance for staff, pupils and all users regarding the use of social media and networking applications.

This policy is designed to protect individual members of staff, pupils and all users.

This policy applies to the use of social media for both business and personal purposes, whether during provision / working hours or otherwise. This policy applies regardless of whether the social media is accessed using provision IT facilities and equipment or equipment belonging to members of staff, pupils or any other IT/internet enabled equipment.

Anyone setting up a social media account that is directly connected to Early Life Enterprise, must follow all the guidelines in this policy.

## 2. Rationale

The widespread availability and use of social media applications bring opportunities to understand, engage, and communicate in new, relevant and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with duties to the provision, the community, our legal responsibilities and our reputation.

The provision use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice. They apply to all members of staff and pupils at the provision.

### The purpose of the policy is to:

- Safeguard all pupils and promote wellbeing
- Ensure users are not exposed to risk as a result of their actions
- Use social media in a respectful, positive and productive way which respects all parties involved
- Ensure that the reputation of Early Life Enterprise staff is protected and that stakeholders understand their ambassadorial role with regard to the provision
- Protect the provision from legal risks
- Ensure that any users are able clearly to distinguish where information provided via social media is legitimately representative of the provision

## 3. Definitions and Scope

The provision defines social media as 'any websites and applications that enable users to create and share content or to participate in social networking'. Social networking sites and tools include, but are not limited to, Facebook, Twitter, Snapchat, TikTok, LinkedIn, Flickr, YouTube and Instagram. It also includes forums and discussion boards such as Yahoo! Groups or Google Groups, online encyclopaedias such as Wikipedia, and any other web sites which allow individual users or organisations to use simple publishing tools.

Many of the principles of this policy also apply to other types of online presence such as virtual worlds.

All members of the provision should bear in mind that information they share through social networking applications, even if they are on private spaces, may be subject to copyright, safeguarding and data protection legislation.

**4. Provision-sanctioned use of social media and/or social media accounts using the name of Early Life Enterprise, the provision logo, or clearly attached to the provision in some way**

There are many legitimate uses of social media within the curriculum, and to support student learning and to share news with the wider community, for example, the provision and sub-departments of the provision have official Twitter, Instagram and Facebook accounts. There are also many possibilities for using social media to enhance and develop pupils' learning and to keep the provision community and our supporters in touch with the provision.

When using provision social media accounts and/or social media accounts using the using the name of Early Life Enterprise, a provision logo, or clearly attached to the provision in some way, the following practices must be observed:

- 4.1.** A distinct and dedicated social media site or account must be set up by the Senior Leadership Team. This should be entirely separate from any personal social media accounts held and should be linked to an official provision email account. Social media accounts must have a link to the Online Safety and Acceptable Use Policy, have official Early Life Enterprise branding and state that it is an 'Official / Provision Approved Site'. If a social media account is identified (that uses the name of Early Life Enterprise, the provision logo, or is clearly attached to the provision in some way) that is not an official provision approved site, this should be reported to the Senior Leadership and Safeguarding team.
- 4.2.** The social media account must be approved by the SLT member and updates to passwords must be shared with the SLT.
- 4.3.** The content of any provision-sanctioned social media site and/or social media accounts using the name Early Life Enterprise, the provision logo, or is clearly attached to the provision in some way, should be entirely professional and should reflect well on the provision.
- 4.4.** Staff must not publish photographs of pupils without the written consent of parents / carers, or the pupil themselves if they are deemed of the age and ability to provide their own consent. Standard practice is to publish only the first name and initial of surname, unless permission has been given by parents or pupils (if deemed of the age and ability to provide their own consent) for the full name to be used. Provision sanctioned social media sites must use images of children in suitable clothing.
- 4.5.** Staff must take into account the Safeguarding Policy when making any posts on provision social media accounts.
- 4.6.** Any links to external sites from the accounts must be appropriate and safe. If they are shared these must be verified as reputable sites. Only appropriate hashtags should ever be used.
- 4.7.** Any inappropriate comments on, or abuse of, provision-sanctioned social media and/or social media accounts using the name Early Life Enterprise, the provision logo, or is clearly attached to the provision in some way, should immediately be removed and reported to the Online Safety Coordinator, Designated Safeguarding Lead (DSL) and the Managing Partner (if appropriate). It is

the responsibility of everyone using the site and social media in general to report abuse immediately.

- 4.8.** All provision sanctioned social media accounts created for provision purposes should include a link in the About or Info page to the Social Media and Online Safety Policies on the provision website. This will indicate that the account is officially sanctioned by the provision.

## **5. Use of social media in practice for staff - for personal and professional use**

- 5.1.** Staff must not have 1:1 communication, including direct messaging (DM), with pupils through any social media, apart from via provision email accounts, Google Meet hangouts via a provision account and provision mobile devices for text messaging. 1:1 communication via Google Meet as part of the Provisions Online Learning.
- 5.2.** Staff should not request or accept any current student of the provision of any age or any ex-student of the provision under the age of 18 as a friend, follower, subscriber or similar on any personal social media account unless they are the parent of the pupil or a close family member.
- 5.3.** It is advisable that staff do not have contact with past pupils (above provision age). Staff may remain in communication with past pupils via a provision email account or the provision social media accounts.
- 5.4.** Any communication received from current pupils on any personal social media sites must be reported immediately to the DSL and to the Online Safety Coordinator.
- 5.5.** If any member of staff is aware of any inappropriate communications involving any student in any social media, these must immediately be reported to the DSLs and to the Online Safety Coordinator.
- 5.6.** Members of staff must ensure that, wherever possible, and where the social media site allows, their privacy settings on social media sites are set so that pupils cannot access information relating to their personal lives or follow them on their personal accounts.
- 5.7.** Members of staff should not specify the provision's name in their workplace, on any social media profiles.
- 5.8.** All email communication between staff and pupils of the provision on provision business must be made from an official provision email account (any deviation from this in an emergency must at once be reported to the line manager). Staff should not use personal email accounts or personal mobile phones to make contact with pupils of the provision, nor should any such contact be accepted, except in circumstances such as provision trips that have been given prior approval by the Managing Partner. Prior approval may also be given by the Managing Partner for staff to communicate professionally with pupils on provision premises for safety reasons.
- 5.9.** Staff must not access any recording systems using personal devices. All recording must be done via provision property/devices.
- 5.10.** Staff should not post or publish on the internet or on any social networking site, any reference to the provision, their colleagues, parents or pupils or discuss pupils or colleagues or criticise the provision or staff. Staff may like, share or make appropriate comment in response to the provision's official social media accounts, in accordance with Section 4.

- 5.11. Staff must not post images on any unofficial Early Life Enterprise social media accounts that includes pupils, unless sharing posts made from a provision official social media account.
- 5.12. Staff are instructed to consider the reputation of the provision in any posts or comments related to the provision on any social media accounts. Reputational breaches by staff are dealt with via the Disciplinary Policy.
- 5.13. Members of staff are responsible for overseeing and monitoring any social media account attributed to their area of responsibility where the social media account is using the name of Early Life Enterprise, the provision logo, or clearly attached to the provision in some way.

## 6. Guidance and advice for staff

Most common social networking sites are inherently insecure places to have discussions which contain any sensitive information. Privacy laws can be violated, and the reputation of our provision can be damaged if the public sees a discussion of any sensitive information taking place on social networking. Staff should be aware that these types of cases can result in disciplinary action.

Any Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed outside working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of breaching this policy will be required to co-operate with an investigation, which *may* involve accessing of *relevant* passwords and login details in some circumstances. This would be in accordance with any policies affecting the monitoring of electronic communications and in accordance with an employee's legal rights.

Judgement as to what specific examples constitute inappropriate use will be made by the Managing Partner of the provision on a case-by-case basis taking into account the circumstances of the case, reasonableness, what risks could reasonably be known at the time the offence took place and consistency.

Examples of cases which have involved disciplinary action or dismissal have involved:

- Posting comments on Facebook about pupils or their parents which are inappropriate and in some cases have divulged personal information.
- Commenting about other colleagues at work or inappropriate messages sent to them which could constitute harassment, discrimination, victimisation or bullying.
- Posting comments about personal views of issues in the public domain which could lead the provision and its community to lose confidence in the employee, for example racist comments
- Joining groups which may be deemed to be inappropriate for employees of the provision or city council to be members of
- Inappropriate relationships with pupils arising from social media

The policy is not intended to restrict all employee activity on social media however provision representatives are asked to exercise caution and professional judgement about what they use it for, who they communicate with and subject matter.

Provision representatives are advised to make full use of the security settings available within the systems but note that these cannot be guaranteed to provide protection against allegations being made or disciplinary action being taken.

## **7. Use of social media in practice for pupils**

- 7.1.** Pupils use of social media on any Provision IT systems, Provision Managed Chromebooks and Provision IT (Google) accounts accessed at any time (including during online learning) and equipment/devices and any personal devices (including hand held devices, watches or any other internet enabled device) brought on to the provision site or at a provision activity, must comply with the Pupils' Computer/Device Usage Agreement and the Provision's Online Safety and ICT Acceptable Use Policy. Pupils should also follow any additional code of conduct / guidelines put in place for online learning from home.
- 7.2.** Pupils must not access any social media that is for adults only or if the pupil does not meet the minimum age requirement.
- 7.3.** Anonymous sites must not be accessed as there is a high risk that inappropriate comments can be exchanged, causing distress or endangerment.
- 7.4.** Bad, including offensive, explicit or abusive, language and inappropriate pictures must never be included in messages.
- 7.5.** All messages should be positive and not include anything that could be upsetting or defamatory towards others or the provision.
- 7.6.** Pupils must take responsibility for keeping details of their accounts private, using full privacy settings and logging off properly and not allowing others to use their accounts.
- 7.7.** Pupils must report anything offensive or upsetting that they see online to the appropriate bodies, either by using the "report abuse" tabs or by speaking to their parents or a member of staff.
- 7.8.** It is a serious offence to use another person's account, or to create an account in another person's name without their consent.
- 7.9.** Pupils should not regard anything posted online as private and should remember that harassment, defamatory attitudes and racism are just some issues which could lead to prosecution.
- 7.10.** An individual's "Digital Footprint" is becoming increasingly significant when it comes to job applications. If unfortunate decisions are made it will be extremely difficult, perhaps impossible, to eliminate the evidence.
- 7.11.** If pupils see inappropriate postings by other pupils, they must inform the provision so that steps can be taken to avoid possible repercussions.
- 7.12.** The Malicious Communications Act applies to social media interaction by pupils, staff and parents of the provision.

**7.13.** Pupils must have permission from the Managing Partner for any social media accounts using the name of Early Life Enterprise, the provision logo, or clearly attached to the provision in some way.

## **8. Use of social media in practice for parents**

- 8.1.** Positive contributions to the Provision social media, such as Twitter, are welcomed.
- 8.2.** Any concerns or issues about the provision, its pupils or staff should be expressed directly to the provision and not be voiced on social media.
- 8.3.** Parents must obtain permission before posting pictures that contain other parents or their children, unless sharing or liking a post from the provision's official social media account.
- 8.4.** If parents become aware of inappropriate use of social media by their own or other people's children, they should contact the provision so that the provision can work with the parents to educate young people on safe and appropriate behaviour.
- 8.5.** If parents become aware of the inappropriate use of social media by other parents or provision staff, they should inform the provision so that steps can be taken to remedy the situation.

### ***Proprietary Information***

Staff may not share information which is confidential and proprietary about the provision. This includes information about services, programmes, financial, strategy, and any other internal confidential, proprietary, or sensitive workplace information that has not been publicly released by the provision. These are given as examples only and do not cover the range of what the provision considers confidential and proprietary. If staff have any questions about whether information is proprietary, they must speak to their Line Manager or SLT member before releasing it. Staff must also be aware of the points made within their employment contract when they joined the provision, a copy which can be obtained from HR.

The provision's logo may not be used without explicit permission from the Managing Partner; the provision owns the rights to all logos, mottos and phraseology and their usage.

### ***Workplace Privacy***

The provision respects staff member rights to privacy and to express themselves. However, the provision and staff members must also respect, and diligently protect, the privacy of fellow staff members, pupils, parents, and others. Privacy and confidentiality must be maintained in every possible way.

Staff must not discuss pupil or family related information via social networking and public social media, texting, or online unless it is an approved medium and for a provision related purpose. Staff are advised to be extremely cautious in conversations with other staff, parents and volunteers in social networking, on the basis that privacy laws can be violated even if a person's name is not shared.

The provision will honour the privacy rights of current and past employees, current and past pupils and their families, and anyone else associated with the provision, by seeking permission before writing about or displaying internal provision happenings which might be considered to be a breach of their privacy and confidentiality.

### ***Privacy and Security Settings***

The provision recommends staff use security and privacy settings provided by social networking sites. Regardless of privacy settings, staff are advised to be respectful and responsible in all activity if it in any way involves or references the provision, job, or those staff work with.

Staff must understand that on-line content is difficult, if not impossible to retract once posted or sent.

### ***Processing personal data***

Staff members may need to collect and/or share personal data such as parental email addresses, home addresses or parental mobile numbers as part of the remote learning system. As long as this processing is necessary for the provision's official functions, individuals won't need to give permission for this to happen.

However, staff are reminded to collect and/or share as little personal data as possible online and only through the provisions' secure network.

Where information is shared with external agencies this should be done via secure file transfer services or by password protected documents only.

### ***Blogging and Websites***

If staff are developing a website or writing a blog that will mention the provision, staff, Governors, pupils, parents and volunteers, they **MUST** get permission first before writing anything, and advise the Managing Partner they are intending to do this. The Managing Partner may choose to inspect this from time to time.

It is important that staff make appropriate decisions about work-related blogging and the content of blogs, personal websites, postings on wikis and other interactive sites. Staff are advised to use caution with postings on video or picture-sharing sites, or in comments made elsewhere on the public internet and in responding to comments from posters either publicly or via email. If staff are assisting pupils to develop a website or blog, this must first be approved by the Managing Partner or SLT and they must be given password access.

### ***Legal Liability***

Staff should recognise that there is the possibility of being legally liable for something inappropriate which is shared online.

### ***The Media***



If a member of the media or non-traditional online media (including bloggers) contacts a member of staff about the business of the Provision (e.g., programmes, services, pupils, parents, clubs, policies, practices, or additional business information of any kind), the individual must contact the Marketing Department prior to responding.

### **Related Documentation**

Social media should not be used in a way that breaches any of the provision's other policies. This policy refers to and should be read in conjunction with the following documents:

- The Provision's Code of Conduct
- The Provisions Disciplinary Procedure
- Data Protection Policy

### **Raising Concerns**

Other policies and procedures adopted by the provision, such as those covering Whistleblowing, Individual Grievance, Harassment, Discrimination, Victimisation and Bullying (HDVB) should be used to raise any concerns about your treatment at work or any other concerns you may have. The use of social media to raise such concerns will be considered **inappropriate**.

### **Further Guidance**

Further guidance on educating and safeguarding young people online and responding to incidents:

**Sexting** - [UK Council for Child Internet Safety Guidance - Sexting](#)

**Online safety advice for pupils, parents and teachers:** [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) - <http://www.saferinternet.org.uk/> - <https://www.internetmatters.org/>

**Cyberbullying** - [www.childnet.com/cyberbullying-guidance](http://www.childnet.com/cyberbullying-guidance)

**Preventing radicalisation** - [educateagainsthate.com](http://educateagainsthate.com) - [www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation](http://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation)

### **Social Media Restrictions for Social Media Platforms**

What are the age limits for social media apps and platforms?

It is vital that parents, pupils and staff know the age restrictions that are applied to many popular apps. As this is a fast-moving area, we would recommend that parents (with their child) always check before a child accesses an app from an internet safety website such as **Internet Matters**, for which there is a link below. We do not endorse the use of these apps; this information is provided only to help support your children to use social media safely.

<https://www.internetmatters.org/resources/what-age-can-my-child-start-social-networking/>

**SEE BELOW APPENDIX 1**

## Appendix 1

### Social networking standards

Below sets out the standards expected of all staff representatives when using social media

#### DO

- **Act responsibly at all times.** Even if you do not identify your profession or place of work, please be aware that your conduct online could jeopardise any professional registration and/or your employment
- **Protect your own privacy.** Think about what kind of information you want to share online and who you want to share this with. Adjust your privacy settings accordingly.
- **Remember everything is public.** Even with the highest level of privacy settings, once something is online it can be copied and redistributed, and it is easy to lose control of the information. Work on the assumption that everything you post online will be permanent and will be shared with others.
- **Take appropriate action if you are the target of abuse online.** If you are the target of bullying or abuse online you can take action in dealing with this, such as blocking individuals from interacting with you and reporting inappropriate activity.
- **Be considerate to your colleagues.** Pictures or information about colleagues should not be posted on social networking sites unless you have the agreement of the individual concerned. Always remove information about a colleague if they ask you to do so.
- **Respect the privacy of others.** If photographs are taken at an event, then check whether those in attendance expect that any photos may appear on a public social networking site before posting. Remember it may not always be an appropriate way to share information whether work related or not.
- **Remember the benefits.** Used responsibly, social media can be accessed to keep up to date with a number of professions and information.

#### DO NOT

- **Share confidential information online.** In line with the Data Protection Act 1998 employees should not share any child / family identifiable information online or any personal information about colleagues. In addition to this, any confidential information about the provision should not be revealed online.
- **Build or pursue relationships with children, parents, families.** Even if the child / client or parent is no longer within your care, the provision does not deem this as appropriate behaviour. If you receive a request from a child / client or parent, then many sites allow you to ignore this request without the individual being informed to avoid any offence. If you are concerned about this in any circumstance, please discuss with your manager.

- **Use social networking sites to inform professional practice.** There are some circumstances/job roles where this may be appropriate however careful consideration and discussions with management should be applied
- **Discuss work related issue online.** This takes into account conversations about parents, children, colleagues or anything else which may identify the provision online and bring into potential disrepute. Even if you think these conversations have been anonymised, they are very likely to be deemed inappropriate.
- **Post pictures of children/young people/ their parents.** Never post pictures of clients / parents or their children online even if they have asked you to do this. Employees should never take pictures of parents, children unless they are relevant and within the boundaries of the digital images policy. Permission from the subject and parents of children should always be obtained. ***If your mobile phone has a camera then this should not be used in the workplace. (This should be considered depending on the provision's policy for taking digital images)***
- **Raise concerns about your work.** Social networking sites should never be used for raising or escalating concerns at work. If you have concerns then these should be raised through either discussing with your line manager or following the relevant policy/procedure for raising concerns at work.
- **Engage in activities online which may bring the Organisation into disrepute.** Think through what activities you take part in whilst online and what you do or say that may bring the provision into disrepute. Any reports of this will be reviewed in line with their appropriateness.
- **Be abusive to or bully other colleagues.** Social networking sites should not be used as a forum for abusive behaviour towards colleagues.
- **Post derogatory, defamatory or offensive comments about colleagues, the child / parents / clients / families, your work or provision.** Everything posted on a social networking site should be deemed as open to the public and it is therefore unacceptable to use this as a forum for posting inappropriate comments.
- All of the above applies to both open and private sections of any social networking site employees identify themselves with.