SOCIAL MEDIA POLICY AND GUIDANCE

SMBC can provide information in a range of different ways, for example via the use of audio tape, summarising large documents, interpretation, translation and British Sign Language interpreting services.

If you require this information in an alternative format or need assistance because English is not your first language, please contact your nominated Human Resources Advisor in the first instance for further support.

This policy sets out the terms of agreement reached by those participating in the Council's Constitution and Negotiating Framework

Version 6
July 2023

SOCIAL MEDIA POLICY AND GUIDANCE

Current version: 8.0

Document type: Approved Policy

Prepared by: T Slater - Communications
P Sharma – Human Resources

Approved by: **Governance Committee – 27 July 2023**

Review date: **2026**

Circulation: All employees, intranet and extranet

Version	Date	Reason for change
4	April 2016	Policy updated following consultation with trade unions
5	April 2018	Inserted new paragraphs into Section 7 on monitoring due to GDPR changes
6	2023	Scope of prohibited content widened and further guidance offered around appropriate usage on personal pages. New sections added for employees working with children, young people or adults at risk and support for employees facing abuse online.
7	July 2023	Safeguarding policies added to Council policies that underpin this policy
8	July 2023	Council Safeguarding policies outlined and links inserted following Governance Committee meeting

CONTENTS   **PAGE**

1. Introduction

1.1 Social media is a key communications tool for Solihull Council/Maintained Schools, providing an excellent opportunity to reach and engage with a large audience, and this document aims to give clear instructions and guidance on how it should be used by Council/school employees. All employees need to demonstrate acceptable standards of communication and use of social media in both a professional and personal capacity during and outside working hours.

1.2 In this policy and guidance document, we define **social media** to mean:

"Websites and applications that enable users to create and share content or to participate in social networking."

This includes:

- online social networking sites such as Twitter, Facebook Instagram and LinkedIn;
- video and photo sharing websites, for example Flickr, YouTube and TikTok;
- micro-blogging sites e.g. Twitter;
- weblogs, including corporate blogs, personal blogs or blogs hosted by online media publications;
- forums and discussion boards such as Yammer, Google Groups or Yahoo! Groups;
- online encyclopaedias such as Wikipedia;
- internal social media channels and websites; and
- any other websites that allow individual users or companies to use simple publishing tools.

Social media applications are not limited to websites, and this policy and guidance document covers any other electronic application (such as mobile phone based, or handheld device-based applications) enabling information to be shared by user groups or the public at large.

Online communication may include, for example: posting or publishing information using social media applications; uploading and/or sharing photos or images; direct messaging; centralised instant messaging, through cross-platforms such as WhatsApp; status updates; or any other form of interaction and/or communication occurring through social media. The examples listed are non-exhaustive because the social media landscape changes continually, therefore the requirements stated in this document will need to be adhered to whenever new or popular social media sites emerge in the future.

1.3   The aim of this document is to encourage Council/school employees tasked with using social media to do so responsibly and feel confident enough to achieve meaningful results through promoting greater involvement with stakeholders, increased efficiencies and more control over our reputation. All content posted must be in accordance with the requirements stipulated in the Code of Employee Conduct.

1.4   There are risks associated with using social media websites, and the Council/school has identified a number of issues that could lead to both disciplinary proceedings and safeguarding concerns following improper or inappropriate use of such sites by its employees. The Council/school advocates and promotes the online safety of children and young people, and all individuals need to be aware of relevant safeguarding issues because offenders can often target social media sites.

1.5   The following information will make clear the standards that are expected of anyone who works for Solihull Council or a Maintained school and uses social media as well as what action may be taken when it is considered that a member of staff may have breached this policy.

1.6   In addition to employees, the requirements outlined in this policy and guidance document also cover temporary and casual staff, agency workers and volunteers during their time working for and on behalf of Solihull Council or in a Maintained school.

1.7   The Social Media policy and guidance need to be read and understood in conjunction with the following policies:

        Electronic Communications Policy and Guidance
        Data Protection Policy
        Code of Employee Conduct
        Disciplinary Policy
        Resolution Policy
        Recruitment and Selection Policy
        Video Conferencing Guidance
        Corporate Safeguarding Policy

2.   Participating in social media on behalf of the Council

2.1   All requests for social media accounts, pages or profiles should at first be directed to the relevant Head of Service or Head teacher for approval.

2.2   Requests should then be sent to the communications team before an account is created. The communications team will advise on the suitability of the

request, whether the proposed content is more appropriate to any existing Council pages or channels or indicate if it is not acceptable for social media.

2.3 The communications team can provide support and training for any new pages/profiles that are approved.

2.4 The Council's official Twitter account and Facebook page are both managed by the communications team. The communications team will consider access requests to these accounts for a limited period of time (i.e. an event or for a specific campaign), and officers from across the Council/Maintained schools are encouraged to provide the communications team with content for these profiles, either on a one-off or regular basis. The communications team will provide feedback on their effectiveness/response.

Any officers or teams considering getting started on social media who would either like ongoing support or to find out more about social media, should liaise with the communications team.

3. Scope of Prohibited Content

3.1 Any communications made in a **professional capacity** on social media must not either knowingly or recklessly:

3.1.1 bring or cause potential to bring the Council/schools into disrepute; or

3.1.2 place a child, young person or adult at risk of harm.

This could be, for example, by:

3.1.3 making political, defamatory or libellous statements criticising/arguing with colleagues, people who use Council services, residents or any associate of the Council. All activity on corporate social media pages must be non-political;

3.1.4 using offensive or discriminatory language such as swearing, racist or sexist comments, or any other language that could be deemed inappropriate;

3.1.5 uploading, copying or sharing obscene or pornographic material;

3.1.6 publishing any material which is confidential or would breach copyright or data protection principles;

3.1.7 promoting the financial interests or commercial ventures of external companies or organisations, unless prior approval has been obtained by the Head of Service or Head teacher and the communications team has been notified;

3.1.8   discussing matters relating to members of staff or people we support for which social media would not be considered an appropriate forum;

3.1.9   using social media to raise complaints or grievances;

3.1.10   engaging in 'spamming' i.e., publishing the same or similar content repeatedly or in bulk;

3.1.11   accessing links or downloading software on social media pages from unknown individuals or unfamiliar organisations which could compromise the Council/schools in any way;

3.1.12   sharing account passwords with anyone other than the communications team. Account users should not use the same passwords for social media accounts that are used to access Council/school computers or devices;

3.1.13   using social media in any way to attack, insult, abuse, harass, defame or otherwise make negative, offensive or discriminatory comments about Council/school staff, colleagues, people we support or their family members, other professionals, partner organisations of the Council/schools, such as the Voluntary and Community Sector, or any other person;

3.1.14   using any information obtained during the course of work for the Council/school for personal gain or advantage or passing it on to others who may use it in such a way; or

3.1.15   using Council/school email addresses and other official contact details for setting up personal social media accounts or for communicating through such media.

         The above is neither an extensive nor exhaustive list – it provides some examples of what the Council/school considers to be unacceptable and inappropriate. Each case will be dealt with accordingly based on the evidence and information available to consider in relation to the matter, and failure to uphold the standards expected in relation to responsible social media use will result in access to social media facilities being withheld.

3.2   Before sending a post, authors should check that they are confident that the content is appropriate. If any post is issued in error, or a message or response is incorrect, the line manager and communications team must be informed immediately so appropriate remedial action can be taken.

3.3   Plain English should be used to make posts interesting and effective. Council/school jargon and automated feeds need to be avoided so the message can be easily and widely understood.

3.4   Although a conversational tone is encouraged, the subject matter should be directly related to the work of the service area or team that the social media

accounts represent. Content must be seen to fulfil a business function. Information relating to an individual's personal life belongs on their own personal profile.

3.5 Correct spelling and grammar is essential when posting on social media. It looks very unprofessional when a Council/school-affiliated account contains simple spelling errors. Acronyms or abbreviations, which would not be widely understood, and "text language" should be avoided. There is no time limit on social media – users should not feel rushed to type a post, and need to make sure it has been proofread beforehand.

3.6 If there are reasonable grounds to believe an employee has engaged in unlawful activity on a social media site, or has possibly breached any term in this document, an investigation will be instigated which may result in disciplinary action, including potential summary dismissal if warranted by the circumstances. For an agency worker or contractor, this may result in the immediate termination of the assignment. Employees need to use social media appropriately and understand that legal implications may arise through unacceptable use.

The Council/school will act promptly to deal with material that is obscene, profane or signifies harassment. The Council/school will not accept potential liability for an individual's participation on social media irrespective of whether the context is professional or personal. If the law is broken, for example through a defamatory post, the individual/s concerned will be held personally responsible.

3.7 The account owner needs to ensure the accuracy of the information or to ensure that the person asking for the information to be published is authorised to do so. Account owners must regularly review the Council/school accounts they are responsible for. Any inappropriate content must be removed immediately, and the account owner must report the content to their line manager, communications team and directly to the social media site or application.

3.8 Account users need to configure social media accounts to encrypt sessions whenever possible. Facebook, Twitter and others support encryption as an option.

3.9 If a device that is used to access Council/school social media accounts is lost or stolen, the communications team must be notified immediately so that passwords can be changed. If this is a corporate device, ICT must be informed.

3.10 If it is believed that an account has been hacked or infected with a virus or other form of malware (malicious software) or phishing, the line manager, communications team and ICT Services must be notified immediately.

3.11 Posts made on an employee's personal account may be seen by a large number of people and will therefore be deemed public rather than private,

particularly if an association with the Council/school is referenced and may be investigated formally if there are reasonable grounds to suspect the social media Policy and Guidance may have been breached.

3.12   Employees must not represent their personal views as those of the Council/school on any social medium or discuss personal information about people we support, their family members, Council/school members of staff or any other professionals or organisations affiliated with the Authority.

3.13   There are restrictions placed on the nature of publicity that local authorities may issue under the [Code of Recommended Practice on Local Authority Publicity](). Employees or account users should refer any questions or concerns to a member of the communications team to ensure any posted or uploaded content is appropriate.

4.   Social Media during emergencies

4.1   Although social media content is normally sent out during normal office hours there are some exceptions to this, including during a crisis or unusual situations. This will be led by the communications team.

4.2   During these crises (for instance when the Emergency Plan has been enacted or when there is severe weather i.e. snow, localised flooding) users of other Council/school-affiliated accounts are strictly prohibited from sending out their own material regarding the emergency situation.

4.3   This is to ensure the dissemination of consistent and coherent information, verified by appropriate parties, so that overall emergency messaging can be properly controlled to ensure effective communication. Therefore, emergency messages will be sent out from the official Council social media accounts, which can then be shared by other Council/school-affiliated accounts.

5.   Guidance on the use of Social Media

Below is a useful guide for using social media while working at Solihull Council/within Maintained schools.

5.1   **Be honest.** Remember that you are an ambassador for our organisation. Any accounts or profiles that are set up on behalf of Solihull Council/school, are affiliated with the Council/school or post content about Council/school business should be clearly and easily identifiable as corporate profiles. Personal and professional accounts should not be linked.

5.2   **Use a professional tone.** All online conversations should be conducted in a polite, open and respectful manner, even if criticism of the Council/school is

involved. Be prepared for people possibly saying unpleasant things but remember that this is a chance to listen and connect. Be professional and try to encourage constructive criticism and deliberation. Respectfully withdraw from conversations that go off-topic or become profane.

5.3 **Be responsive.** Try to respond to any questions or comments within 24 hours. Offer insights and share what you know and put people in touch with someone who can help if you are not able to. Do listen and provide feedback. Social networks are good listening devices. Forward comments to the right place so that the relevant officers know what is being said. However, make sure you respect confidentiality – do not disclose non-public information or the personal information of others, and do not post content which may embarrass yourself or the Council/school.

5.4 **Use it.** Try to post content on a regular basis. Your audience will soon spot broadcasts and respond accordingly. Accounts which stagnate may need to be deleted if regular and meaningful content is not posted or the information cannot be more easily distributed through other Council/school-affiliated social media. Be confident and don't be scared of participating – an underused account is much worse than no account at all.

5.5 Social media should be linked with business objectives, but will need time, energy and enthusiasm to work successfully. Know what you want to achieve before you start and plan how you will evaluate the success of any social media activity.

6. Branding of Social Media accounts

6.1 Any social media pages/profiles for Council/school services should be branded in line with corporate policy and with the [Code of Recommended Practice on Local Authority Publicity](#)– i.e. pages should be clearly identifiable as part of Solihull Council and should not attempt to give any other impression. Identifying the account with 'SMBC' or 'Solihull MBC' is not recommended because it is not immediately obvious to a member of the public that this would refer to Solihull Council.

6.2 No attempt should be made to create your own Council/school logo for social media (or for any other purpose). All images displayed on social media accounts should conform to the standards expected of all other Council/school communications. For further guidance please contact the communications team or refer to [brand guidelines](#).

7. Publishing photos/videos of people on social media

7.1 It is Solihull Council policy that prior consent must be obtained before publishing on any of our social media channels photographs or videos which contain images of people. Permission needs to be gained from the information owner before publishing any documents, photos, emails and/or reporting on social media any conversations intended to be private, confidential or internal.

7.2 Exceptions to this rule are photos/videos taken of a group of people in a public place. A public place is considered to be, any place where people have no reasonable expectation of privacy (i.e., Solihull, High Street). These photos/videos can be uploaded to social media without getting permission.

7.3 However, although it is not illegal, where a person or several people are clearly the subject of a photograph (i.e., a close up of them or if they fill the majority of the frame) then prior approval must be sought before posting on social media.

7.4 Other people should always be given the chance to move out of a shot/frame before the photo/video is captured and need to have been informed of the intention to post on social media.

7.5 Prior consent from an adult can either be obtained verbally or in writing. Having the subject sign the Council's photographic consent form is preferable, however, logistically, this may not be possible, in which case verbal consent is acceptable though this must be recorded.

7.6 However, it is compulsory to use consent forms for any photos/videos of children. The form should be signed by the parents/guardian of each child whose image has been captured. For photos/videos of schoolchildren, permission should be sought from the accompanying teacher. The consent form and image should then be emailed to comms@solihull.gov.uk for their records.

8. Personal use of Social Media

8.1 Apart from employees who update social media accounts as part of their job role, a certain amount of limited and acceptable personal use of social media is allowed on work computers. If you want to use social media for personal reasons, you are encouraged to do so in your own time either before or after work, during your lunchbreak or other approved break. Usage on personal devices should only take place during breaks from work. Any use of social media on work computers is monitored by ICT, therefore privacy cannot be assumed when using the Council's/school network.

8.2   ICT routinely monitor internet traffic data (websites visited, times and dates of visits etc) to ensure Council/school policies are being adhered to. Periodic reports will be created by ICT so that managers may monitor their employees' use of these facilities. The information obtained through monitoring may be shared internally, including with the employee's line manager, HR and ICT if there are reasonable grounds to believe that there has been a breach of the rules set out in any Council/school policy.

8.3   You need to be aware that such monitoring might reveal sensitive and personal information about you. For example, if you regularly visit social media sites detailing the activities of a particular political party or religious group, then viewing such pages might indicate your opinions or beliefs. By carrying out such activities using the Council's/school facilities you are consenting for the processing of any data about you which may be revealed by such monitoring.

8.4   The information gathered through monitoring will only be retained for long enough to enable any breach of this policy to be detected and a subsequent investigation to be conducted. Any information obtained will not be disclosed to third parties unless the Council/school is under a duty to report such matters to a regulatory authority or a law enforcement agency. More information on monitoring and employees' rights in relation to data can be found in the Council's/school Data Protection policy and Electronic Communications policy and guidance.

8.5   The Council/school does not seek to prevent employees using social media. However, personal accounts should not be used to represent our organisation and should never give the impression that they have permission to do so. The Council/school acknowledges that many employees use social media in a personal capacity, and, while they are not acting on behalf of the Council/school, any information posted may have an impact on the Council's/school reputation.

8.6   Personal and professional profiles should be kept separate. The personal use of social media must neither interfere with an employee's obligation to maintain their professional standards nor impact the reputation of the Council/school.

8.7   If you do wish to engage in conversations about Solihull Council/the school on your personal profile page, you must make it clear that the views expressed are your own personal opinions. It is recommended that you include a statement on every profile you maintain such as: "The views I express here are mine alone and do not reflect the views of Solihull Council/school." However, adding a disclaimer such as this will neither prevent any legal ramifications nor preclude the Council/school from taking appropriate action

in accordance with its policies and procedures wherever necessary. Employees are expected to uphold professional standards at all times, particularly if their role involves interaction with people we support.

8.8   With regard to content that could be inappropriate, or which may affect the reputation of the Council/school, there should be no expectation of privacy, regardless of the privacy settings applied to individual accounts, when posting or uploading content onto social media sites, and views or opinions stated on social media need to be considered as though they are in the public domain. Social networks are cultivated to make sharing information as easy as possible, therefore any content, even within a setting apparently limiting and restricting access to the public at large, may ultimately end up being copied, shared and redistributed widely and come very quickly to others' attention (i.e. colleagues, managers, Elected Members or people we support).

8.9   Stating that views are merely personal opinions does not justify making any comments which may damage the Council's/school reputation. Officers in politically restricted posts should pay particular-attention to what they post on their personal social media profiles, because the effect of including a local authority employee on the list of politically restricted posts is to prevent such an individual from having any active political role either in or outside the workplace. The Council/school as an organisation cannot be seen to directly promote any political party or messages.

8.10   It is good business practice for organisations and members of staff to keep certain topics confidential by refraining from speculation on the future of the Council/school or the way it operates and keeping topics focussed to matters of public record when speaking about the Council/school or local government. Confidential Council or business information must not be loaded onto a corporate social media site or a personal profile.

8.11   Employees communicating or interacting in a **personal capacity** on social media must not:

- bring the Council into disrepute, for example by:
  - criticising or arguing with service users, people we support, colleagues or Elected Members;
  - making disparaging or adverse comments about the Council/school or its partners;
  - browsing, downloading or posting offensive images or links to inappropriate, discriminatory or illegal content;
  - exposing the Council/school to potential civil or criminal liability through a breach of legislation; or
  - undermining the integrity or impartiality of the Council/school
- breach confidentiality, for example by:

- o divulging sensitive Council/school information;
- o revealing confidential information about an individual (such as a colleague or individual we support) or organisation; or
- o discussing detail regarding Council/school operations that has not been released to the public, such as work being undertaken with a customer/client or its future strategic/business plans
- breach copyright, for example by:
  - o using without permission someone else's images or written content that are subject to copyright protections; or
  - o failing to give due acknowledgement where permission has been provided to reproduce something.
- do anything that could be considered discriminatory against any individual, for example by:
  - o making offensive, derogatory comments or posting defamatory content relating to any of the protected characteristics covered under the Equality Act 2010; or
  - o using social media to bully or harass another individual, such as an employee of the Council/school

The above list is neither extensive or exhaustive and employees may be required to remove posts considered to be in breach of the policy and guidance.

8.12   Any questions or concerns should be directed to a member of the communications team to ensure any posted or uploaded content is appropriate.

8.13   The communications team needs to be alerted if a potential issue is spotted on social media of which the Council/school needs to be aware or where an official Council/school response is needed.

9.   Guidance for employees working with children, young people or adults at risk

9.1   In addition to the aforementioned, employees in roles working with children, young people or adults at risk should act in accordance with any statutory requirements and service protocols applicable to their position and take heed of any guidance issued by regulatory bodies such as the Health Care Professions Council or Ofsted. The content of messages on platforms such as WhatsApp may not only lead to the loss of employment but also result in professional disciplinary proceedings against any regulated professionals involved in the behaviour.   Receiving offensive material via messaging services such as WhatsApp, staying in a group in which it is being circulated and not reporting fellow regulated members can all lead to charges of professional misconduct. Employees should therefore:

- only use Council/school approved accounts and equipment to communicate with people we support;
- refrain from accepting or initiating 'friend' requests or partaking in private online contact with children, young people, adults at risk or any of their family members in order to maintain clear professional boundaries;
- understand that anything posted online, including photos, images and video material, could leave themselves vulnerable to scrutiny, affect their reputation and potentially be classed as misconduct or gross misconduct;
- respect the rights of the children, young people or adults at risk they are protecting, but act upon any concerns potentially compromising the safety of vulnerable people by following appropriate safeguarding procedures;
- show discretion in all personal communication on social media and check that private security settings are maintained on personal accounts by only granting access to friends or followers or on profile pages; and
- avoid displaying personal information and consider asking friends to reflect before uploading photographs which may cause embarrassment.

9.2   All employees must undertake mandatory safeguarding training to understand the Council's/school safeguarding policies and their responsibilities as Council/school employees. There is regular Safeguarding training delivered as part of continued professional development (CPD).

10.   Support for employees receiving online abuse

10.1   In order to provide a welcoming forum for other users to engage with our platforms, the Council/school reserves the right to mute or block individuals, who post comments that contravene the principles outlined in this document, by filing a report through the relevant channels to block their account and escalating the issue directly with the company. Every social media platform has a procedure for reporting users who violate their code of conduct. In extreme cases, social media content may be referred to the police for investigation.

10.2   Cyberbullying, uninvited, intimidating, or offensive comments designed to attack, threaten or belittle an individual, and trolling, inflammatory comments intended to provoke arguments and confrontation, can be distressing to experience. It is advisable to avoid entering into discussions with someone posting abuse. Employees should also avoid replying to messages on behalf of others, as they could end up being subjected to harassment, too.

10.3   Online harassment can create feelings of frustration, isolation and anxiety, therefore, if an employee believes they are suffering from cyberbullying, trolling or feels offended by material uploaded by a colleague on any digital communication network, they should discuss the situation with their line manager or a HR Advisor for support.

10.4   Cyberbullying and trolling are as unacceptable as any other form of bullying or harassment, and will be addressed wherever applicable under the Council's Disciplinary policy.

11.   Employee Assistance Programme

11.1   Additionally, the EAP (Employee Assistance Programme) can be accessed to address the toll online abuse can induce and recommend ways to engage in anxiety-reducing practices.   The service gives employees a place to turn to for support any time of day or night, 365 days a year. To use the confidential service, you can contact the freephone number 0800 028 0199, the email facility on their website or the instant webchat facility at www.healthassuredeap.co.uk using the following login details:

Username: Solihull
Password: MBC

11.2   There is also the **'My Healthy Advantage' Mobile App** and an Online Health & Wellbeing Portal which offers employees access to online webinars, factsheets and tailored programmes online, allowing them access to support independently or alongside their counselling support. The 'My Healthy Advantage' app provides an enhanced set of wellbeing tools and features designed to improve your mental and physical health by using personal metrics to set goals and achievements. It is available on the Apple Store and Google Play store and you will need to use the **employer code which is MHA109491**.

11.3   The EAP helpline is also available to line managers to offer support when dealing with challenging managerial situations. Their advisors do not advise on HR policies and procedures but can provide a facilitative and supportive space to help assist them with complicated or difficult issues. Some managers may want to rehearse a conversation, talk through how their own issues are impinging on a work problem or voice concern about their ability or confidence to manage a workplace conflict or difficulty. To use the service, managers can contact the freephone number **0800 028 0199.**

11.4   There can be times when additional support is needed for employees and managers alike. Experienced, professional counsellors are available and can determine appropriate resources and help with the next steps. Where there

is deemed to be a clinical need, up to 6 face-to-face or telephone counselling sessions can be offered to employees.