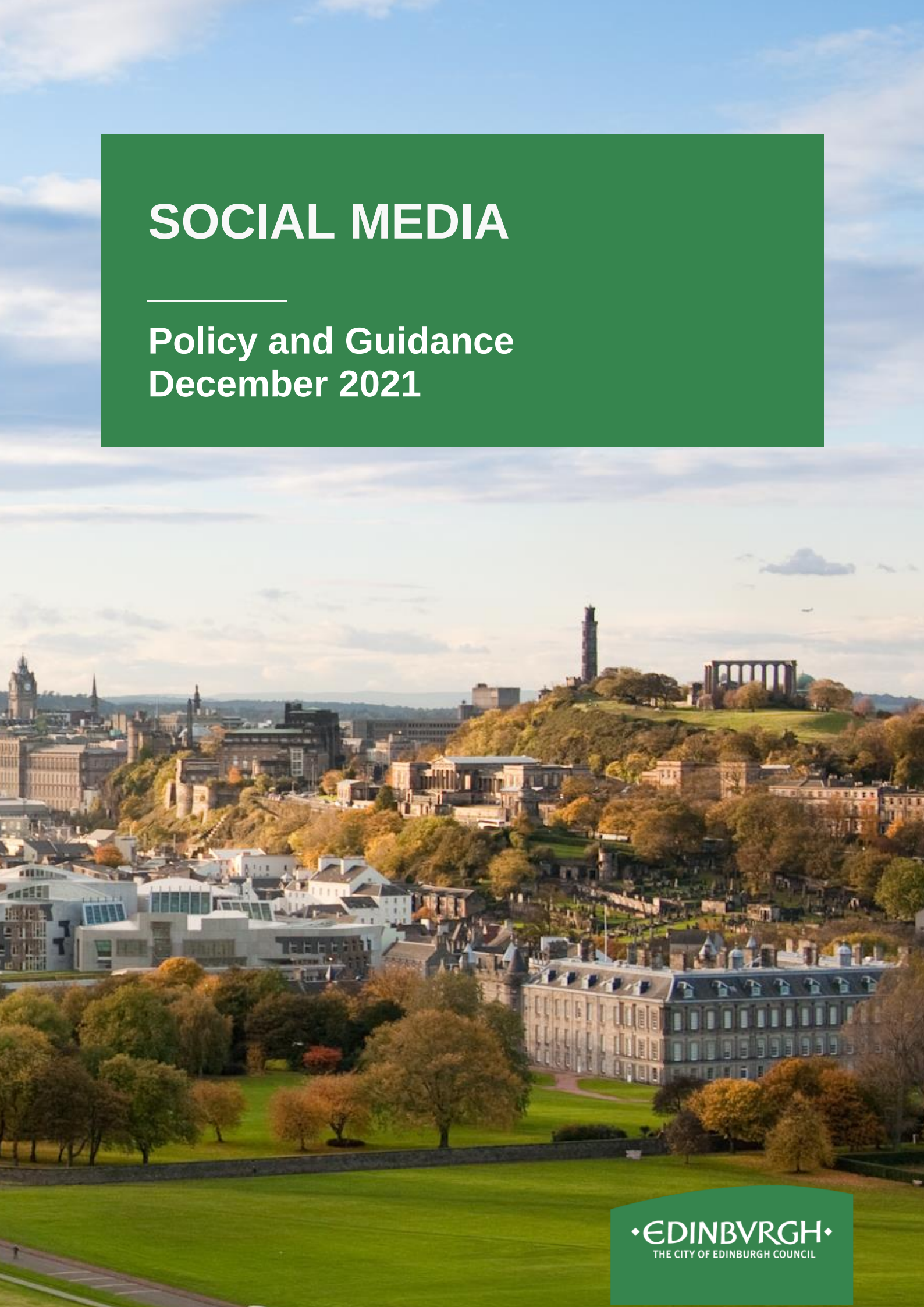
SOCIAL MEDIA

Policy and Guidance
December 2021



EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Contents

Introduction

There are enormous benefits to using social media. It helps us to communicate with the public in real time, to consult and engage, and to be more transparent and accountable.

As a council, we're taking a 'digital first' approach and social media plays a vital role in the way we communicate with residents, businesses and stakeholders in Edinburgh.

But it also presents potential risks for the Council. Our social media accounts reflect our values and policies publicly and if not managed correctly, can undermine the reputation of the entire organisation.

So, alongside all the benefits that social media can bring, we must be aware of the responsibilities that come with it and make sure we maintain the highest level of propriety.

Our social media policy and guidelines

We want you to feel supported and confident with using social media, but we also need to make sure you know how to protect our reputation, our legal obligations, our information and our systems.

These guidelines outline the approaches and processes City of Edinburgh Council social media accounts must follow to make sure we are appropriately managing these risks.

Please note that this guidance isn't designed to offer social media best practices, or guidance on how to get the most out of your social media accounts – you can find this in our training materials.

Here are the key points we'll cover in these guidelines:

- Your role and responsibilities.
- Training.
- Protecting your account.
- Looking after personal data and our legal obligations.
- Managing the Council's reputation.

Scope and related policies

Social media are websites and applications that enable users to create and share content or to participate in social networking.

Examples of popular social media sites include, but are not limited to: LinkedIn, Twitter, Facebook, YouTube, Instagram, Snapchat, Flickr, Wikis and blogs, Whatsapp, TikTok.

These guidelines describe your obligations as a manager of, or a contributor to, an account or profile on a social media site operating on behalf of the Council. This includes any account run by a service, department, school, building, project, group or other function which sits within the Council. These accounts are considered to be owned and operated by the Council.

They don't apply to your use of personal social media accounts. Appropriate personal social media use is covered in our ICT Acceptable Use Policy. You should ensure you're familiar with the policy if you're using a personal social media account.

If you have a 'professional' social media account - an account where you represent yourself in your professional capacity at the Council, for example as a senior manager using social media to communicate the work of your department - these guidelines don't apply to your ownership and use of that account. However, you should make sure you understand your obligations under the ICT Acceptable Use Policy, and be aware of the reputational importance to the Council of appropriate use of your account.

If you have a question about professional accounts and ownership, you can contact communications@edinburgh.gov.uk

These guidelines supplement the City of Edinburgh Council's ICT Acceptable Use policy, Code of Conduct and other HR policies.

The ICT Acceptable Use policy already sets out clear guidance on the use of the internet and what might constitute misuse or unacceptable behaviour. Colleagues should make sure that they are familiar with the relevant areas of the policy when they are considering how they might make use of social media.

Your role and responsibilities

We have a collective responsibility to make sure the way we're using social media protects against damage to our reputation, compromise of our systems or data, or breach of our legal obligations.

To do that, it's important that you understand your individual responsibilities, and the responsibilities of others.

In these guidelines, we'll set out your general responsibilities as well as the individual responsibilities of:

- **Account managers** (colleagues who own a Council social media account)
- **Contributors** (colleagues who contribute to Council social media accounts)
- **Support teams** (colleagues who develop guidance, training and policy for Council social media accounts)

These guidelines will refer to these roles throughout. You should identify the role you have and your associated responsibilities. Where the guidance doesn't refer to a role, it will apply to both account managers and contributors.

General responsibilities

Be professional, responsible and respectful

All posts from our social media accounts represent the Council. It's vital that messages posted are carefully considered, appropriate and do not damage the reputation of the Council or otherwise bring it into disrepute. Mistakes can happen, but you should put safeguards in place to minimise that risk, such as checking content with a colleague before publishing.

All content posted or promoted on our accounts must be courteous and respectful of others. Our accounts mustn't be used to criticise or argue with colleagues, customers, partners, or any other individuals or organisations.

Stay impartial and politically neutral

The standards expected of you as an employee of the Council are covered in our Code of Conduct**.** The Code says we must be impartial and politically neutral, and this extends to our communications and use of social media.

'Pre-election period' is the time between the announcement of an election and polling day and, during this period, there's heightened sensitivity around ensuring that public resources are not used in any way that might prejudice the result of an election. These obligations apply to our communications year-round but, when in a pre-election period, you should take extra care to ensure that any content on your social media account is clearly and directly relevant to the service or issue being discussed and reflects an agreed council decision or policy.

Remember that, beyond what you post, many of your actions on social media such as 'liking' or 'commenting' will be visible to others in the social media community.

If you have any questions or concerns, you can speak to our Communications team or Elections team.

Understand the social media platforms you're using

Social media platforms are evolving at a dramatic speed - the way users consume content is changing and emerging threats to platforms such as increased regulation and users' need for privacy will continue to change platforms in the years to come.

It's important, therefore, that you continue to adjust your approach as platforms change and new norms emerge. Stay focused on your objectives, be willing to learn and make every effort to be accessible, integrated and responsive with your online community.

Protect the information we hold

These guidelines cover many of the steps we need to take to make sure that we're looking after the data we collect and the data we hold. Make sure you understand what you need to do to look after our customers' data and to keep your account safe.

Account managers

All Council social media accounts must have a designated 'manager'.

The account manager is responsible for looking after the day-to-day operations of the account and ensuring the account is operating appropriately, in line with these guidelines, and all other relevant policies.

If you're an account manager, you're responsible for the management and ongoing governance of the account - including administration of all 'contributors'. You should make sure all contributors have appropriate access and have completed the relevant training before they work on the account.

All Council social media accounts must have a current Council employee as an active, designated account manager. A record of the account manager should be held by Communications alongside the account business case. If there's a need to change the registered account manager, in addition to any other actions required, Communications should be provided with details of the new account manager for the account as soon as possible.

Communication regarding Council-wide social media initiatives, guidance, training opportunities or changes to the policy will be via social media account managers who should share the information with account contributors as needed.

Contributors

Contributors are colleagues who aren't social media account managers but otherwise access or directly contribute to a Council social media account. This may be through posting publicly on the account but could also be accessing it to extract data or view information within the account.

If you are a social media contributor, you should make sure you understand the guidance in this document and how to apply it to your role on the relevant account.

Support teams

Support teams are responsible for the development of suitable guidance, governance, training and policy to help colleagues using social media on behalf of the Council do so with the knowledge and understanding they need. Support teams include the Communications team, ICT security, Information Governance and Human Resources.

Training

All account managers and contributors must complete 'Social Media' training on myLearning Hub before using social media on behalf of the Council – this is essential for any users of social media on behalf of the council. This course supplements these Social Media Guidelines and offers an introduction to social media use.

For account owners

You should carry out a yearly training needs assessment for yourself and all contributors to the account. This assessment should consider whether you have the core competencies to use social media effectively and safely, and if not, what steps should be taken to fill your knowledge gaps.

Core competencies

All social media users should:

- Understand their own role and responsibilities when using social media on behalf of the council, including:
    - how data should be managed and processed
    - securing their account
    - their legal obligations
    - their role in a major incident or emergency

- Understand the social media platform they are using, including best practices for publishing, engagement and account management.

Identifying knowledge gaps

You should consider whether you and any other contributors have any gaps in these competencies and consider how they might be filled.

You should review the training and guidance available and, if you feel you still have knowledge gaps, speak to the communications team about training and support that could be developed. We'll provide training and guidance, where needed, to help you to make the most effective use of social media.

Protecting your account

Who has access

For account owners

It's vitally important that you limit access to your account to those who actively need to use it, and remove anyone who no longer needs access.

If a colleague with access to your social media account leaves the Council (or even changes roles), make sure their access to the account is revoked. This needs to be done promptly, before they move. Doing this should form part of your wider process to manage 'joiners, movers and leavers'. Additionally, if a colleague isn't changing roles or leaving the organisation but no longer needs access for any other reason, their access should be removed until they need it again.

If you're using shared passwords and a contributor leaves, you should immediately change the account password outside of your regular password changing schedule.

Some social media platforms (such as Facebook) allow users to be given different levels of access. For example, this can allow a user to post to the account but not amend its settings, or to view an account to export data but not post to the account. Access should be given at the minimum level needed for the contributor to carry out their role.

For contributors

Your account manager should remove your access if you no longer need it. However, if this isn't done or you still have access through alternative means (such as separate social media tools), you should make your account manager aware and arrange for the access to be removed.

Passing on the management of your account

For account managers

If you're an account manager and are moving to a new role in the Council, leaving the organisation or are no longer best placed to manage your account, you must take steps to pass the account on to a new manager.

If there's a suitable replacement account manager in your team, you must:

- Provide them with all master passwords and administrative access they require. This should be done securely, in a password-protected document or encrypted email, for example.
- Remove any administrative access you have.
- Inform communications about the change in account manager by emailing communications@edinburgh.gov.uk

If there's no current suitable replacement account manager, you can pass ownership over to the Communications team until one can be identified.

If, because of your change in role, your account is no longer viable, you should make sure it is properly closed down.

Social media management tools

For account managers

If you have multiple contributors to your account(s), social media management tools can offer a number of security and operational benefits.

A tool can centralise your social media activity, helping with your planning and collaboration, reporting and removing duplication of effort.

Additionally, social media tools allow improved security of your account by removing the need to share master passwords or give direct access to social media accounts to contributors.

There will be a monthly or yearly financial cost to using a social media management tool. You should consider using a social media tool if you have multiple contributors and your budget allows.

You can find out more about the tools available, as well as costs, what they can do and get started with a social media tool, by getting in touch with the Communications team.

Passwords and account security

It's very important that we control the access to our social media accounts to make sure that only authorised colleagues can publish content and view what's in our social media accounts.

For account managers

The first step in securing your account is making sure you have set appropriate and strong passwords. Passwords should be set up, changed and stored in line with the Council's password policy.

Some social media platforms (such as Twitter) primarily operate using a single master password. Other platforms (such as Facebook) use 'Page roles' where a personal social media account is granted access to the business page, and passwords are therefore managed separately by each user.

As an account manager, you're responsible for maintaining and controlling the use of master passwords and/or page roles for your account.

Most social media platforms contain additional security features such as two-factor (or multi-factor) authentication. Using two-factor authentication for social media access is one of the most secure ways to operate business/organisational accounts and you should use this whenever it is available. It works by adding an additional layer of security on top of your

password, requiring you to present another form of identification in addition to the password, such as a code that's texted to a registered phone.

If you use a social media management tool, the same processes should be followed for its passwords and access. If you've connected a social media tool to your social media account but it's no longer being actively used, you should remove the access it has to your social media account.

The National Cyber Security Centre also has useful guidance on how to protect accounts that you manage.

If a contributor (or anyone else with authorised access) is publishing damaging content or taking any inappropriate action on your account, you need to make sure you're able to quickly revoke their access. If you're using shared master passwords, you should immediately access the account and create a new password. This will logout all other users. If you're using a platform that has 'page roles' you should immediately revoke the access of the user.

If your account is 'hijacked' by someone without authorised access, your priority should be regaining control of the account to contain any damage, before then trying to correct any malicious content that's been posted. You will most likely be unable to login to your account to change your password - if so, you should contact the Communications team immediately, and start to follow the account recovery process for your platform:

- Twitter
- Facebook
- Instagram
- LinkedIn
- YouTube

Don't wait until you're in the middle of a real incident - think about the steps you'll need to take to regain control of your account, and make sure you have access to everything you need to do it quickly in order to minimise any damage caused.

For contributors

As a contributor, depending on the social media platform you're accessing, you may be using a shared password or you may be accessing it via your own account with your own password.

If you're using a shared password, you have a responsibility to store it safely and use it in a way that reduces the risk of it being used by someone who isn't authorised to do so. This means not keeping your password in a place (either digitally or physically) that can be easily read or accessed, avoiding using 'auto-fill' settings and not using on devices that are shared.

If you're using a platform that allows you to set your own personal password, you should follow the Council's password policy. Additionally, if the platform has two-factor (or multi-factor) authentication available, you should use it to protect your account.

The National Cyber Security Centre also has useful guidance on how to manage the security and privacy settings on your accounts.

If you see any activity on your account that seems suspicious, you should let your account manager know as soon as possible so they can take steps to secure your account.

Looking after personal data and our legal obligations

This guidance is focused on our legislative obligations on social media and supplements the legal provisions you should be aware of that are outlined in our ICT Acceptable Use policy. You should make sure you've read and understood all of them as they apply to your use of social media.

Personal data

If you own or contribute to a Council social media account you have a direct way of communicating with customers, businesses and many of our stakeholders. Because of that, you have a responsibility to make sure the audience you're communicating with understands how we process their personal data, and that you handle any personal data you do receive appropriately.

The legislation we need to follow when processing personal data is the General Data Protection Regulation (GDPR) and the Data Protection Act. The GDPR requires that personal data must be processed securely using appropriate technical and organisational measures. You can find more information about the GDPR on the orb.

Personal data is information that relates to an identified or identifiable individual. If a person can be identified from the data, or if the data is a unique reference or identifier of one person, then it will likely fall into the definition of personal data. Examples of personal data include, but aren't limited to, a person's: name, address, email address, pupil record or service request (where individuals are identified). You can find more information about what is personal data on our Information Governance team's Info Note on the orb.

For social media, one of the challenges we face is that social media technologies aren't currently designed to reasonably create, retain and dispose of personal data sufficiently well, in a way that allows us to practically meet our legal obligations.

Therefore, you shouldn't receive or store any personal data through your social media account.

The only exceptions to this are social media accounts operated by the Council's customer care team, and photography, video or audio you use on your social media account. You can find out more about how you must use photography that includes personal data, below. If you think you need to receive or store personal data through your social media account, you should contact our Communications and Information Compliance teams.

Photography

If you're planning to take photographs, video or audio recordings to use on your social media account, you must get consent from the people who feature in these as they are considered 'personal data' under the GDPR.

You can find a form that you can use to obtain consent, on the orb.

Additionally, you must:

- decide how long you will keep and use the photo, video or audio files for and delete the files at the end of that time.
- keep a record of all the photos and video and audio recordings and of the people who have consented. You should keep these records alongside your consent forms.
- allow people to remove their consent at any time. If they do, you must make sure that their files are removed from your collection and your social media account, and not used again.

You can find more information about getting and keeping permissions on the orb.

If your photography, videos or audio doesn't contain people, there are no personal data considerations needed.

For account managers
You're responsible for making sure you have appropriate processes in place to obtain and store consent to allow you to meet your obligations under the GDPR. Consent must be stored centrally, not with individuals. For example, you must still be able to remove a photograph despite the contributor who obtained the original consent no longer working for the Council.

Data protection impact assessments

A Data Protection Impact Assessment (DPIA) is a process to help us identify and minimise data protection risks. We have completed these for each social media platform the Council currently operates on. You should make sure you've read and understood the DPIA for each platform you are using.

- Twitter
- Facebook
- Instagram
- LinkedIn
- Nextdoor

If you wish to use a platform that we haven't assessed, please detail that in your New Account request and be aware that we'll need to complete the assessment before your account can be set up.

Privacy notice

Individuals have the right to be informed about the collection and use of their personal data.

One of the ways we do this is in a Privacy Notice, where we explain our purposes for processing personal data, our retention periods for that personal data, and who it will be

shared with.

We must make sure that our audience on social media is able to access our privacy notices by always including a link to the website that stores them on our social media account pages. For Council services, privacy notices are stored at www.edinburgh.gov.uk/privacy.

For account owners

Even if you don't plan on processing any personal information, you must make sure that your social media account links to a website that holds the privacy notice for your service. The link doesn't need to be directly to your privacy notice - you can link to a page that provides more information about what you do for example, as long as they can then navigate to a privacy notice on the website should they wish.

Copyright and other legal obligations

Your legal obligations are covered in full in our ICT Acceptable Use policy, but there's a couple that you should be particularly aware of on social media:

- **Copyright**. You must respect copyright when using images or other online material. You should assume that any material or works you want to distribute or display via social media is protected by copyright unless you can specifically demonstrate otherwise. Resharing using functionality built-in to the social media platform (such as 'retweet' or 'share' buttons) is permitted.

- **Freedom of Information (FOI).** You should be aware that what you say on a social media platform, even if you make the message private, may be subject to access legislation such as FOI.

Managing the Council's reputation

New social media accounts

If your objective is to reach as many people as possible, or to get your messages out to as much of your audience as possible, setting up new social media platforms can be appealing.

However, there are a few things to consider. Firstly, while different or emerging platforms may have an impressive number of users, it's important to consider whether those people are part of the audience you need to reach. A tailored and targeted approach will often outperform mass 'broadcasts' to an ill-defined audience.

Another consideration is investment. You need to have the resource in place to manage a new channel and make it a success. You'll need a well-maintained process for creating content and to ensure you're engaging with your community in a timely way. Running one channel well, where you have established yourself already, is better than running five channels less well.

If you do decide you'd like to adopt a new platform, even if it's similar in its aims and approach as the platform you already have, you must go through the new account approval process.

It's very important that we have a strategic and well-considered network of social media accounts across our services. They should be valuable assets to us, getting the most out of the time and effort we give to them, and allowing us to offer a cohesive and consistent range of social media accounts to our audience(s). All new accounts must demonstrate clearly that they fill a role that isn't already served elsewhere and have a strategic plan for how they will operate.

For account managers
If you set up a social media account that represents the Council but hasn't been authorised, it must be immediately closed and you should follow the new account process. If you have an account that predates our formal social media authorisation process (i.e. setup prior to 2015) you should contact the Communications team so that we add your account to our central record of authorised accounts.

Closing accounts

For account managers

Sometimes social media accounts reach the end of their useful life and you need to make a decision about whether they should continue to operate.

It might be that the account isn't growing or you aren't reaching enough people through it, you might no longer be able to justify the time involved in its day-to-day operations, or the reason the account was set up (for a project or initiative, for example) no longer applies.

If this happens, rather than let the account lapse, which doesn't reflect well on us reputationally, we need to make sure we close them appropriately and efficiently.

To close your account, there are a few steps you should follow:

- Let the Communications team know about your intention to close the account. Depending on your account, there might be instances where your account could be repurposed for another role or it could be worthwhile holding on to the username for the account.

- Once you've received confirmation that the account can be closed, you should communicate that to your audience. Importantly, you should let them know where they can go to get more information on your service or subject area - this might be via our website or another social media account. Depending on the platform, you may want to post this a few times so your audience doesn't miss it.

- Once you've allowed time for your audience to see your closure message, you can delete (or deactivate) your account. Here's how to do that on:

    - Twitter
    - Facebook
    - LinkedIn
    - Instagram
    - YouTube

- Finally, you should audit your digital and non-digital materials (such as websites, email footers, printed letters or flyers) to remove any links and references to your closed social media page.

Verification

Many social media platforms offer the ability for accounts to be verified.

The meaning of verification can differ between platforms but it generally signifies that this is the authentic account for the public figure, organisation, celebrity or global brand that it represents. For us, there are benefits to being verified on social media as it can reassure users that they are engaging with the Council and not a spoof or fake account.

The criteria for having your account verified is different for each social media platform and can often change. If your account meets the criteria, verification isn't guaranteed and is at the discretion of the social media platform.

For account managers

You should consider whether your account(s) can be verified.

Here's how to apply for verification on:

- Twitter
- Facebook

- Instagram
- YouTube

If you are unsuccessful, you can still take steps to reassure users that your account is the official representation of your organisation, department, building or project. You should make sure your profile is complete, with professional imagery and a clear bio that states who you are, what you do and links to an official Council website. Additionally, your content should be professional and in line with the expectations of your audience.

Fake and 'spoof' accounts

One of the reasons to verify our social media accounts is to give residents, businesses and all of our stakeholders in Edinburgh confidence that they're engaging with us, and not anybody else.

Free access and the short time it takes to set up a social media account means that, on many social media platforms, there are problems with fake accounts, bots and accounts used for trolling. Bots and fake accounts are covered in 'Interacting with your audience'. Fake accounts fall into two main categories; here's how to deal with each:

- **Fake accounts that aim to impersonate your account.** These accounts present a risk to us reputationally as they may purposefully issue false or misleading information. Additionally, they may be a vehicle for fraud by attempting to obtain personal or sensitive information. These accounts should be reported to the social media platform immediately:
    - Twitter
    - Facebook
    - Instagram
    - LinkedIn
    - YouTube

- **Spoof or satire accounts.** These are accounts that aim to impersonate us in a humorous way. These accounts are allowed on Twitter, subject to them meeting certain requirements. It's unclear what Facebook, Instagram, LinkedIn and YouTube's official policy is on parody accounts. If you think there's a risk that users may believe the parody account to be genuine, you should report it to the platform immediately.

Interacting with your audience

Social media is fundamentally a two-way conversation. Once you start using social media to talk to your audience, you have to be a part of the conversation, especially when people are asking you questions. If you don't have the resource to answer queries, then it's likely you don't have the resources to use the channel.

Dealing with detractors

As soon as you become active on social media, it's likely that you're going to encounter 'detractors'.

Detractors (or 'trolls') typically talk to you on social media in a derogatory and/or offensive way without good reason. You should be careful not to confuse detractors with people who have valid complaints or questions.

There are several ways to deal with detractors. If the user has a complaint or question but is posing it in an unacceptable way, you can refer them to our Social Media Acceptable Use policy which explains our standards for engaging on social media.

If criticism you receive is especially aggressive or inconsiderate, initially it's probably best to refrain from responding.

However, we support the right of our colleagues to mute or block people on social media who are threatening or abusive. You should consider banning or blocking a user as a last resort. But if a user continually breaks our acceptable use policy or is abusive, you can take action to report and/or block them.

Social media platforms have different tools available to do this:

- Twitter
- Facebook
- Instagram
- LinkedIn
- YouTube

Bots

Bots are social media accounts that operate in a partially or fully autonomous fashion, but are typically designed to mimic human users.

Some bots are used for good but, unfortunately, most are used in dishonest or unhelpful ways. The most common type of bot you're likely to experience are 'spam' bots, which spread links to commercial websites, but you could also encounter others, such as those designed to artificially amplify the popularity of a person or movement.

Some signs of a bot are a profile that's incomplete (lack of photo, for example) and the user is posting very frequently and/or is excessively repeating the same text or content.

Identifying bots can be tricky. However, if a user that's engaging with you is clearly a bot, you should use the tools available on the platform to report and block them.

Social media in a major incident or emergency

Social media can be an extremely useful tool in the Council's emergency management, with real-time updates providing up to the minute guidance and advice.

However, it's vitally important that the information we do share is timely, consistent, credible and accurate.

Major incidents

A major incident is a significant emergency that requires the implementation of special arrangements by one or more of the emergency services, the NHS or us as the Local Authority. An example of this would be a terrorist threat.

During our crisis response, our focus will be on the speed and effectiveness of our initial response. The effective use of our social media tools will be critical during this phase to engage our networks to gather, analyse and disseminate information promptly.

If we are involved in a major incident, there's a number of ways you can support our communications.

- Your networks can be an extremely useful way for our messages to reach as many people as possible - please reshare relevant messages from us and our partners.

- It's important that all of our messages are clear and consistent - you should immediately review any 'scheduled' social media activity (posts that will automatically be sent in the future) and consider removing/postponing them

- If you have your own information to share, it's important that it's clear, timely and accurate. Information can spread incredibly quickly in a crisis situation and it can be very difficult to regain control of the message if a mistake happens. If you need guidance, you should speak to the communications team or your senior manager before posting.

Minor emergencies or sensitive issues

For minor emergencies, such as bad weather or a local incident, you should consider how you can further support our core messaging with information relevant to your audience. You could offer updates on your services if they're affected, for example.

A sensitive issue might be the death of a public figure, or an incident that isn't directly affecting the City or our services. If this happens, you should use judgement to consider what's appropriate to post to your account. You should review any scheduled social media activity and agree on an approach for any future posts with all contributors. Scheduled posts that don't reflect the situation can be taken as insensitive and can cause unintended reputation damage.

Further guidance and support

Social media has always been a fast-paced world - platforms are continually developing, new features released and algorithms evolving.

When you create content for social media you should follow the latest best practice, but understand that best practices can change quickly as the platforms themselves change.

It's therefore important to keep watching, listening and learning. You should evaluate and improve your approach as you go.

Useful places to find the latest developments in social media platforms are their blogs:

- Twitter blog
- Instagram blog
- LinkedIn blog
- Facebook blog

If we change our social media policy and guidance, we'll contact account managers to let them know.

For more information about anything you've read here, or for anything else on social media, you can get in touch at communications@edinburgh.gov.uk