Matrix of social media guidelines for journalists

	The New York Times Social Media Guidelines (2017)	BBC News Group Social Media Guidance for Staff (2015)	Social Media Guidelines for AP Employees
Refrain from expressing partisan opinion or political affiliations on your social media accounts as this could affect not only the reporter but the media organization as source of fair and balanced news.	In social media posts, our journalists must not express partisan opinions, promote political views, endorse candidates, make offensive comments or do anything else that undercuts The Times's journalistic reputation. Our journalists should be especially mindful of appearing to take sides on issues that The Times is seeking to cover objectively.	Where individuals identify themselves as being linked with the BBC, or are programme makers, editorial staff, reporters or presenters primarily associated with the BBC, their activities on social media have the potential to compromise the BBC's impartiality and to damage its reputation.	Employees may not include political affiliations in their profiles and should not make any postings that express political views. AP staffers must be aware that opinions they express may damage the AP's reputation as an unbiased source of news. AP employees must refrain from declaring their views on contentious public issues in any public forum and must not take part in organized action in support of causes or movements.
Be mindful that posts you publish on "private" accounts may not necessarily remain public. Consider that almost anything you share online, no matter the privacy settings placed, might go public.	We consider all social media activity by our journalists to come under this policy. While you may think that your Facebook page, Twitter feed, Instagram, Snapchat or other social media accounts are private zones, separate from your role at The Times, in fact everything we post or "like" online is to some degree public. And everything we do in public is likely to be associated with The Times.	Disclaimers written in biographies such as 'my views not the BBC's' provide no defence against personal expressions of opinion on social media that may conflict with BBC guidelines. Individuals involved in the production or presentation of any output in News or other factual areas that regularly deal with a range of public policy issues have a particular responsibility to avoid damaging the BBC's impartiality.	Employees should be mindful that any opinions or personal information they disclose about themselves or colleagues may be linked to the AP's name. That's true even if staffers restrict their pages to viewing only by friends. We recommend customizing your privacy settings on Facebook to determine what you share and with whom. However, as multitudes of people have learned all too well, virtually nothing is truly private on the Internet. It's all too easy for someone to copy material out of restricted pages and redirect it elsewhere for wider viewing.
Also consider that the friends you add, the pages you like, and the posts you like and share might be perceived as something you subscribe to or endorse. Balance is key to minimize perception of partisanship or bias.	Avoid joining private and "secret" groups on Facebook and other platforms that may have a partisan orientation. You should also refrain from registering for partisan events on social media. If you are joining these groups for reporting purposes, please take care in what you post.	Where our official accounts follow others, we should ensure that we reflect due impartiality in our choice of accounts to follow - similarly if our official accounts share or like content originally published by others.	It is acceptable to extend and accept Facebook friend requests from sources, politicians and newsmakers if necessary for reporting purposes, and to follow them on Twitter. However, friending and "liking" political candidates or causes may create a perception among people unfamiliar with the protocol of social networks that AP staffers are advocates. Therefore, staffers should try to make this kind of contact with figures on both sides of controversial issues. We should avoid interacting with newsmakers on their public pages – for instance, commenting on their posts.
	If you are linking to other sources, aim to reflect a diverse collection of viewpoints. Sharing a range of news, opinions or satire from others is usually appropriate. But consistently linking to only one side of a debate can leave the impression that you, too, are taking sides.	Expressions of opinion on social media can take many forms – from straightforward tweets or updates, sharing or liking content, following particular accounts or using campaigning or political hashtags. If for example a member of staff repeatedly likes or shares, without comment, content reflecting a particular point of view on a matter of public controversy it might create the impression that an individual agrees with that view. Likewise if a member of staff only follows social media accounts reflecting one point of view on a matter of public controversy that might create a similar impression.	Retweets, like tweets, should not be written in a way that looks like you're expressing a personal opinion on the issues of the day. A retweet with no comment of your own can easily be seen as a sign of approval of what you're relaying. However, we can judiciously retweet opinionated material if we make clear we're simply reporting it, much as we would quote it in a story. Introductory words help make the distinction. These cautions apply even if you say on your Twitter profile that retweets do not constitute endorsements. Many people who see your tweets and retweets will never look at your Twitter bio.
Be polite and respectful when talking to people on social media as in any other conversations. Avoid engaging in hostile discussions.	Always treat others with respect on social media. If a reader questions or criticizes your work or social media post, and you would like to respond, be thoughtful. Do not imply that the person hasn't carefully read your work. If the criticism is especially aggressive or inconsiderate, it's probably best to refrain from responding. We also support the right of our journalists to mute or block people on social media who are threatening or abusive. (But please avoid muting or blocking people for mere criticism of you or your reporting.)	Staff should also not post offensive or derogatory comments or content on social media and avoid abusing their position as a BBC employee in personal interactions.	AP is strongly in favor of engaging with those who consume our content. Most feedback we receive is constructive, and any substantive criticism of our content should be taken seriously, however it may be phrased. However, it's best to avoid protracted back-and-forth exchanges with angry people that become less constructive with each new round. Abusive, bigoted, obscene and/or racist comments should be flagged to the Nerve Center immediately and, if appropriate, to AP Global Security (contact dspriggs@ap.org).
Always alert the newsdesk first on breaking news events for guidance before sharing on any social media platform.	We believe in the value of using social media to provide live coverage and to offer live updates. But there may be times when we prefer that our journalists focus their first efforts on our own digital platforms. We generally want to publish exclusives on our own platforms first, not on social media, but there may be instances when it makes sense to post first on social media. Consult your supervisors for guidance.		AP journalists have live-tweeted news events on several occasions with great success.*
Erroneous social media posts should be avoided at all cost but if an error is committed, and a post need to be taken down for it, a new post should explain the circumstance of the take down.	Be transparent. If you tweeted an error or something inappropriate and wish to delete the tweet, be sure to quickly acknowledge the deletion in a subsequent tweet. Please consult our social media corrections policy for guidance.	We should also be transparent about errors, corrections and apologies as a result of any mistakes we make on our branded social media accounts. We should ensure we connect the correction or apology clearly with original error. If in doubt consult social media leads or Editorial Policy.	Twitter.com allows us to delete tweets we've sent. Deletion, however, removes the tweet only from Twitter.com and perhaps some other Twitter clients. Tweets of ours that have been retweeted or reposted elsewhere will still remain publicly visible. If you believe a tweet should be deleted, contact a Nerve Center manager to discuss the situation. Erroneous tweets or other social media posts need to be corrected as quickly and transparently as errors in any other AP service. This applies to AP-related tweets or posts on personal accounts as well. The thing to do is to tweet or post that we made a mistake and explain exactly what was wrong.
Journalism is a practice of verification. Avoid sharing unconfirmed and unverified content.	Exercise caution when sharing scoops or provocative stories from other organizations that The Times has not yet confirmed. In some cases, a tweet of another outlet's story by a Times reporter has been interpreted as The Times confirming the story, when it in fact has not.		Staffers should always refrain from spreading unconfirmed rumors online, regardless of whether other journalists or news outlets have shared the reports; because of staffers' affiliation with AP, doing so could lend credence to reports that may well be incorrect.
Safety is of utmost importance. Consider that there might be activities on social media that could compromise or threaten the safety of journalists, their colleagues, and the subjects they work with.	If you feel threatened by someone on social media, please inform your supervisors immediately. The Times has policies in place to protect the safety of our journalists.		Staffers must not post on social networks any information that could jeopardize the safety of AP staff — for example, the exact location of staffers reporting from a place where journalists may be kidnapped or attacked. This also applies to reports of the arrest or disappearance of staffers. In some cases, publicity may in fact help a staffer, but this determination must be made by AP managers handling the situation.
Sources and information found on social media should be vetted as is the practice in regular circumstances.			It can be difficult to verify the identity of sources found on social networks. Sources discovered there should be vetted in the same way as those found by any other means. If a source you encounter on a social network claims to be an official from a company, organization or government agency, call the place of business to confirm the identity, just as you would if a source called on the phone.
Finally, observing the ethical guidelines is still very much encouraged.	In addition to these social media guidelines, staff members should be familiar with and follow the newsroom's Ethical Journalism guidelines, which apply here as well.	Social media platforms provide an invaluable opportunity for both BBC output and staff to share content and engage with others in an informal environment. But just as everything we do on our own platforms is informed by the Editorial Guidelines, so is all our activity on social media platforms – whether it is in a 'professional' or 'personal' or capacity.	AP's Social Media Guidelines are based on our Statement of News Values and Principles.

	Facebook	Twitter
Location Data Facebook users restrict location history tracking for mobile devices while on Twitter, location information for posts can also be restricted.	Settings ⇢ Location ⇢ Location History.	Settings ⇢ Privacy and Safety ⇢ Tweets ⇢ Location information
Facial Recognition Facebook users can opt out of the facial recognition capacity.	Settings ⇢ Face Recognition.	
Photo Tagging Photo tagging for both Facebook and Twitter can be restricted and disallowed, respectively. While other Facebook users may still be able to tag users in posts and photos, this can be restricted and users can choose to filter which ones appear in their timeline. In a tagged post, users can also have the tag removed. Meanwhile, for Twitter, users may still be tagged in posts with photos.	Settings ⇢ Timeline and Tagging	Settings ⇢ Privacy and Safety ⇢ Tweets ⇢ Photo tagging
Two-Factor Authentication For added security, both Facebook and Twitter users can choose to turn on the two-factor authentication feature where users will be asked to enter a special login code acquired through various means like through an SMS, an authentication app, or a physical security key	Settings ⇢ Security and Login ⇢ Two-Factor Authentication.	Settings ⇢ Account ⇢ Security ⇢ Two-factor authentication
Log in details Facebook and Twitter keep a record of locations where and devices used to log into the platforms. Users can review this record and see suspicious login instances even logout of them immediately.	Settings ⇢ Security and Login ⇢ When You're Logged In.	Settings ⇢ Privacy and safety ⇢ Personalization and data ⇢ See your Twitter data ⇢ Apps, devices & information ⇢ Connected apps ⇢ Apps and sessions
Login alerts Facebook users can setup alerts about logins from unrecognized devices or browsers while Twitter sends push notifications and email alerts detected suspicious logins or logins to new devices for the first time.	Settings ⇢ Security and Login ⇢ Setting Up Extra Security.	Twitter sends push notifications and email alerts if they detect a suspicious login or when logging into new devices for the first time.
Privacy Facebook's privacy settings allows users to choose which posts other users can see, who can send friends requests, see a user's friend's list, look up a user using their email address or phone number, and whether or not users will allow to be indexed in search engines outside of Facebook. While Twitter users can choose to allow if they could be found on the platform through their email and phone number, display media that may contain sensitive content, choose to set accounts to private, and control how Twitter personalizes content, collects and shares certain data about the users.	Settings ⇢ Privacy	Settings ⇢ Privacy and security
Other services Facebook and Twitter accounts can be used to login to other connected online services like Whatsapp and Instagram for Facebook and Periscope for Twitter. Other services are also available inside and outside the platform like games, online payment, and many others. Users can review and revoke access of apps and services to the data of Facebook and Twitter users.	Settings ⇢ Apps and Websites Settings ⇢ Instant Games	Settings ⇢ Privacy and safety ⇢ Personalization and data ⇢ See your Twitter data ⇢ Apps, devices & information ⇢ Apps, devices & information/ Connected apps
Off-platform activities Of services outside of Facebook where a user's account is used to connect and login, Facebook keeps a list of off-Facebook activities or information shared with the platform. This can be reviewed by users.	Settings ⇢ Your Facebook Information ⇢ Off-Facebook Activity.	
Download Personal Data Facebook and Twitter users can request to download the information of users generated on the platforms.	Settings ⇢ Your Facebook Information ⇢ Download Your Information	Settings ⇢ Privacy and safety ⇢ Personalization and data ⇢ See your Twitter data ⇢ Download an archive of your data
Uploaded Data Mobile applications of Facebook and Twitter can upload the contacts list of users. Facebook has a function which can continuously upload the user's contacts to the platform. Users can check, revoke contacts uploading, and delete contacts uploaded on these platforms.	On your mobile app: Settings and Privacy ⇢ Settings ⇢ Media and Contacts Check contacts uploaded to Facebook: https://www.facebook.com/mobile/facebook/contacts/?tab=contacts	Settings ⇢ Privacy and safety ⇢ Discoverability and contacts ⇢ Manage contacts
Data generated for ad targeting Ads that Facebook and Twitter users see on the platform are based on the data gathered from their activities and information provided. Users can, although limited, review and limit personal data shared with advertisers.	Settings ⇢ Ads	Settings ⇢ Privacy and safety ⇢ Personalization and data ⇢ See your Twitter data ⇢ Interests and ads data ⇢ Interests from Twitter/Inferred interests from partners/Tailored audiences