

SOCIAL MEDIA POLICY

USE OF SOCIAL MEDIA AT WORK

Employees are only permitted to log on to social media websites for private purposes using the Diocese of Chester (DBF) IT systems and equipment outside their normal working hours (for example, during lunch breaks or after the working day has finished) and this must not under any circumstances interfere with their job duties or have a detrimental effect on their productivity. The Diocese of Chester nevertheless reserves the right to restrict access to this type of website at any time.

However, employees may be asked to contribute to the Diocese of Chester's own social media activities during normal working hours, for example by managing a Facebook account or running an official Twitter account for the Diocese. Employees must be aware at all times that, while contributing to the Diocese of Chester's social media activities, they are representing the Diocese.

THE DIOCESE OF CHESTER'S SOCIAL MEDIA ACTIVITIES

Where employees are authorised to contribute to the Diocese of Chester's own social media activities as part of their work, for example for marketing, promotional and recruitment purposes, they must adhere to the following rules:

- use the same safeguards as they would with any other type of communication about the Diocese of Chester that is in the public domain
- ensure that any communication has a purpose and a benefit for the Diocese of Chester
- obtain permission from their line manager before embarking on a public campaign using social media
- request their line manager to check and approve content before it is published online
- follow any additional guidelines given by the Diocese of Chester from time to time.

The social media rules set out below also apply as appropriate.

SOCIAL MEDIA RULES

The Diocese of Chester recognises that many employees make use of social media in a personal capacity outside the workplace and outside normal working hours. While they are not acting on behalf of the Diocese of Chester in these circumstances, employees must be aware that they can still cause damage to the Diocese of Chester if they are recognised online as being one of its employees. Therefore, it is important that the Diocese of Chester has strict social media rules in place to protect its position.

When logging on to and using social media websites and blogs at any time, including personal use on non-Diocese of Chester computers outside the workplace and outside normal working hours, employees must not:

- other than in relation to the Diocese of Chester's own social media activities or other than where expressly permitted by the Diocesan Secretary, write about their work for the Diocese of Chester unless it is of a purely factual nature and not confidential
- post views that could be linked to the Diocese of Chester unless they ensure that any personal views expressed are clearly stated to be theirs alone and do not represent those of the Diocese of Chester
- conduct themselves in a way that is potentially detrimental to the Diocese of Chester or brings the Diocese of Chester or its clients, contractors or suppliers into disrepute, for example by posting images or video clips that are inappropriate or links to inappropriate website content
- other than in relation to The Diocese of Chester's own social media activities or other than where expressly permitted by the Diocesan Secretary, use their work e-mail address when registering on such sites
- allow their interaction on these websites or blogs to damage working relationships with or between employees and clients, contractors or suppliers of the Diocese of Chester, for example by criticising or arguing with such persons
- include personal information or data about the Diocese of Chester's, clients, clergy, contractors or suppliers without their express consent (an employee may still be liable even if employees, clients, clergy, customers, contractors or suppliers are not expressly named in the websites or blogs as long as the Diocesan Secretary reasonably believes they are identifiable) - this could constitute a breach of the Data Protection Act 1998 which is a criminal offence
- make any derogatory, offensive, discriminatory, untrue, negative, critical or defamatory comments about the Diocese of Chester, its employees, clients, clergy, customers, contractors or suppliers (an employee may still be liable even if the Diocese of Chester, its employees, clients, clergy, customers, contractors or suppliers are not expressly named in the websites or blogs as long as the Diocesan Secretary reasonably believes they are identifiable)
- make any comments about Diocese of Chester's clergy or employees that could constitute unlawful discrimination, harassment or cyber-bullying contrary to the Equality Act 2010 or post any images or video clips that are discriminatory or which may constitute unlawful harassment or cyber-bullying - employees can be personally liable for their actions under the legislation
- disclose any trade secrets or confidential, proprietary or sensitive information belonging to the Diocese of Chester, its employees, clients, clergy, customers, or contractors or breach copyright or any other proprietary interest belonging to the Diocese of Chester, for example, using someone else's images or written content without permission or failing to give acknowledgement where permission has been given to reproduce particular work - if employees wish to post images, photographs or videos of their work colleagues or clients, clergy, customers, contractors or suppliers on their online profile, they should first obtain the other party's express permission to do so.

Employees must remove any offending content immediately if they are asked to do so by the Diocesan Secretary.

Employees should remember that social media websites are public fora, even if they have set their account privacy settings at a restricted access or “friends only” level, and therefore they should not assume that their postings on any website will remain private.

Employees must also be security conscious when using social media websites and should take appropriate steps to protect Diocesan social media sites.

Should employees notice any inaccurate information about the Diocese of Chester online, they should report this to their line manager in the first instance.

SOCIAL MEDIA MONITORING

The Diocese of Chester reserves the right to monitor employees’ use of social media on the internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected. The purposes for such monitoring are to:

- promote productivity and efficiency
- ensure the security of the system and its effective operation
- make sure there is no unauthorised use of the Diocese of Chester’s time
- ensure that inappropriate, restricted or blocked websites are not being accessed by employees
- make sure there is no breach of confidentiality.

The Diocese of Chester reserves the right to restrict, deny or remove internet access, or access to particular social media websites, to or from any employee.

CONTRAVENTION OF THIS POLICY

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under The Diocese of Chester’s disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee’s summary dismissal.

APPENDIX 1

PROTECTING YOURSELF WHEN USING SOCIAL MEDIA: A GUIDE FOR CHURCHES AND CHURCH LEADERS

The Church is the original social network – it connects people, encourages them to participate and to reach out to others. We can use social media and e-communications as a Church to enhance our identity and community, learning and communication, mission and ministry. But alongside these opportunities are also risks: social media increases and accelerates the positive and negative aspects of any communication. These guidelines are designed to help a range of people think through how they use these tools in the life of the Church.

The online world has changed the way we communicate and while it has many advantages and the mission possibilities are clearly there to grasp there are a number of traps and risks that have led to individuals getting into a great deal of trouble and potential disciplinary action. If you want to engage with this media, we want to make sure you don't fall into the trap of becoming a figure of notoriety.

This guide has been written to help clergy, readers and lay workers protect themselves online. We encourage people to engage people, develop Church life and promote the Gospel of Christ through social media, but we want you to get it right.

This guidance note gives information about protecting yourself from the risks of entering the online debate. It sets out the best practice for making sure you can build safeguards around your communication – and any communications you conduct on behalf of your church or church group.

As a church leader you are a public figure – even if that is just in your own local context – and you have to be aware that your comments and opinions will be watched, valued, scrutinised and criticised.

The Diocese of Bath and Wells have issued 9 commandments to which we have added a 10th as a summary of some basic rules to apply when you use Social Media.

THE DIOCESE OF CHESTER 10 COMMANDMENTS

1. Don't rush in
2. Remember updates are transient yet permanent
3. You're an ambassador for the church
4. Don't hide behind anonymity
5. Think about the blurring of public/private life boundaries
6. Safeguarding: communicating directly online is like meeting someone in private
7. Stay within the legal framework
8. Respect confidentiality
9. Be mindful of your own security
10. Our mission purpose is to direct people to look at God and not ourselves!

A BRIEF GUIDE TO WHAT'S OUT THERE

There are many internet social media tools that can be used. The most common are:

Blogging sites: these are personal websites or online diaries. You posts thoughts and musings alongside links to other areas you are interested in. Others can comment on your posts - this can lead to debates.

Facebook: This is the most well known and used social media site. Here you can build networks of friends and join pages dedicated to particular areas of interest. People use Facebook to organise events, launch campaigns or simply keep in touch. It is similar to having several conversations about things that interest you.

There are other similar sites – LinkedIn, Ning, MySpace, Tumblr, Whatsapp, Snapchat, Instagram and Pinterest for example – that do similar things for different audiences.

All these sites can link to each other and can include videos and photos.

Twitter: This is known as a micro-blogging site where users follow people or organisations that interest them and are followed in turn. On twitter users post short 140 character messages (tweets) to their followers but can also send private messages. You can also include links to pictures and other sites in a similar way to Facebook.

Flickr: This is a website for sharing photos where users can upload and share pictures. You can also search for photos

YouTube and Vimeo: These are websites for sharing videos and are organised in a similar way to Flickr. You can add comments to videos (and others can comment on your work).

Discussions and forums: Many websites have discussion boards and forums for debate and comment – these are particularly popular for news based sites

What we are talking about

The main emphasis of this document is to do with Facebook and Twitter – however this advice applies to any tool where you may put information, comment or opinion.

THE KEY THINGS YOU CAN DO TO PROTECT YOURSELF ONLINE

There are a few simple things you can think about and do to protect yourself and your posts

- You are a public figure
- You must remember that you are a representative of the Bishop and of the church and your opinion and behaviour matters. People will look to what you do and say either for moral guidance or to find the true you. As a result the unguarded and off the cuff remark can very often take on extra significance. In particular anyone in ordained or licensed ministry needs to remember their oaths of Canonical Obedience to the Bishop and their vows to offer their lives as an example to others in ministry.
- Social media blurs the distinction between the professional and private life of any individual. It is easy to think that you can have an element of privacy online. You can't. You can protect yourself by remembering at all times you are a public figure.

- Think about your friends and followers. You need to think about who you accept as friends on Facebook (and to a certain extent followers on twitter). Reaching out to a wide network of people who may share different views and express them in colourful ways may have many benefits. But you may need to think through the challenges of reaching a diverse group of people online and how you disassociate yourself from those who may cause you embarrassment. Similarly your friends may not appreciate your public position and post messages, photos or videos that could be very harmful. You could also be “tagged” in these photos bringing more attention. One example is the many incidents of teachers’ careers getting into trouble because of the embarrassing holiday or night out picture. Some people consider having a professional and personal online persona. This can manage some of the risk but shouldn’t be seen as the ultimate solution.
- Anything you say is in the public domain. You may think you are speaking to a controlled private group of friends but anything you put online can be regarded as published. Even if you put safeguards around whom you accept as friends or followers information can still be passed on.
- Legally posts may be subject to action under the laws of libel and defamation and online activity also has implications for Data Protection and copyright law. You cannot necessarily protect yourself by being anonymous or using a pseudonym. Legal cases have forced anonymous posters to reveal their identity.
- Clergy have found themselves the centre of unfavourable media attention after they posted social media comments. Most notably the Bishop of Willesden was suspended for comments about the Royal Wedding. A clergyman in the north criticised aspects of worship and was widely criticised and rebuked. Your comments may not reach the same level of harm but if you criticise an aspect of your local church, parishioners or simply sound off at the end of a stressful day your comments could be taken and used against you. It may be regarded as a disciplinary matter if you make any derogatory comments about others on any social media site. You can protect yourself by only putting comments that you would also make in a public meeting; in your parish magazine or in local media.
- Anything you say is permanent. You may be able to delete a comment or entry made in haste but records could still have been seen. Your comment could have been reposted or copied to other sites. Even if you sent a direct message or personal email the recipient could find a variety of ways to keep a valid record of the comment. People could take a screen dump to save information that you may have thought is deleted.
- Your opinion matters. Everyone has an opinion and it is good and important to have debate. Freedom of speech is important and the church has a duty to hold a mirror up against society and society’s values. Many do this through a blog (online diary). This is fine provided that you make clear the source of the opinion. It seems a bit of a modern cliché but you do need to state that views expressed are your own views and not necessarily that of your local or the national church. Many people put that statement on their twitter feed.
- You need to remember that a large part of people’s interest in what you say comes from the authority your membership of the church gives. You may be speaking for yourself but people will make assumptions about who you are speaking for. This is particularly true if you are a member of a forum or representative group. You need to be aware when you may have a conflict of interest. You also need to consider those issues you need to remain publically neutral about.

- You also need to be extremely careful if you are using as a profile your church or church group. Then any opinions have to be those of the group and not your personal opinion.
- Pictures tell a thousand words. Be careful about any pictures or videos you post. They may seem innocuous and fun to you but many people have fallen foul with the image of an unguarded moment. You may be “tagged” by a friend in photos that you don’t wish to be seen in. You need to make sure they are removed.
- Don’t forget copyright. It’s easy to use Google to search and find that relevant image as a background to a blog entry or post. But beware that many images are protected by copyright and some organisations will pursue infringements. Similarly you need to be sure of the copyright of any music or film you wish to use.
- Online safeguarding is of essential importance. You need to be very aware of making sure you are safe, public and open in your communication with people – particularly the vulnerable. You need to have regard to our diocesan policies and the law. You should think very carefully about accepting “friend requests” from young or vulnerable people and in no circumstance should initiate a request with a vulnerable person. In any communications you should not attempt to send a direct message to a vulnerable person - all communication online should be open and transparent.
- Similarly you need to respect other people’s confidentiality. It is easy to share someone else’s story as an illustration of a point you wish to make. But you may not have that right (even if you change details). Make sure you are not the source of confidential information leaking out.
- Think about your personal details. You need to keep yourself safe and not publish any personal or contact details – particularly addresses or phone numbers unless you are happy for people to know them.
- The single biggest thing you can do to protect yourself online is to assume anything you put is in the public domain and will be shared. If you do that and self edit your comments you are approaching the medium in a clear, responsible manner.

WHO TO CONTACT FOR ADVICE AND SUPPORT

Stephen Freeman

APPENDIX 2

PROTECTING YOURSELF WHEN USING SOCIAL MEDIA : A GUIDE FOR CHURCH HOUSE AND CHESTER DIOCESAN STAFF

The Church is the original social network – it connects people, encourages them to participate and to reach out to others. We can use social media and e-communications as a Church to enhance our identity and community, learning and communication, mission and ministry. But alongside these opportunities are also risks: social media increases and accelerates the positive and negative aspects of any communication. These guidelines are designed to help a range of people think through how they use these tools to build up the wider life of the Diocese of Chester.

The online world has changed the way we communicate and while it has many advantages and the mission possibilities are clearly there to grasp there are a number of traps and risks that have led to individuals getting into a great deal of trouble and potential disciplinary action. If you want to engage with this media, we want to make sure you don't fall into the trap of becoming a figure of notoriety.

This guide has been written to help the staff of Church House and the diocese who are invited to represent the Diocese of Chester online, to protect themselves. We encourage people to engage people, develop Church life and promote the Gospel of Christ through social media, but we want you to get it right.

This guidance note gives information about protecting yourself from the risks of entering the online debate. It sets out the best practice for making sure you can build safeguards around your communication – and any communications you conduct on behalf of Church House and the diocese. You have to be aware that your comments and opinions will be watched, valued, scrutinised and criticised.

The Diocese of Bath and Wells have issued 9 commandments to which we have added a 10th as a summary of some basic rules to apply when you use Social Media.

THE DIOCESE OF CHESTER 10 COMMANDMENTS

1. Don't rush in
2. Remember updates are transient yet permanent
3. You're an ambassador for the church
4. Don't hide behind anonymity
5. Think about the blurring of public/private life boundaries
6. Safeguarding: communicating directly online is like meeting someone in private
7. Stay within the legal framework
8. Respect confidentiality
9. Be mindful of your own security
10. Our mission purpose is to direct people to look at God and not ourselves!

DIRECTIVES ABOUT WHAT YOU MIGHT / MIGHT NOT DO ONLINE

The Diocesan Facebook and Twitter accounts allow the various departments to target key audiences, deliver key messages and engage the wider Diocese. The Diocesan Secretary, The Archdeacons, the Director of Communications, and Heads of Department, and certain others are given authority to post on behalf of the DBF on these accounts.

Posts should be relevant, provide useful information, promote the work of Church House and the wider Diocese in line with our objectives.

Posts should follow established policy and should only be in line with the officer's area of responsibility.

Posts might share interesting third party content eg from para-church organisations, where this is in line with our objectives and is appropriate and impartial.

Posts should take into account cultural sensitivities and avoid posting anything that could be considered offensive by anyone who may read the post online.

Avoid comments of a party political nature. This is especially true at election times. (Seek advice if you are unsure.)

Online debate should only clarify issues and never result in protracted argument.

Do not post or share anything which breaches copyright.

Do not disclose any information that is confidential.

If using personal social media accounts you should still remember that you are a DBF (or diocesan) employee.

A BRIEF GUIDE TO WHAT'S OUT THERE

There are many internet social media tools that can be used. The most common are:

Blogging sites: these are personal websites or online diaries. You post thoughts and musings alongside links to other areas you are interested in. Others can comment on your posts - this can lead to debates.

Facebook: This is the most well known and used social media site. Here you can build networks of friends and join pages dedicated to particular areas of interest. People use Facebook to organise events, launch campaigns or simply keep in touch. It is similar to having several conversations about things that interest you.

There are other similar sites – LinkedIn, Ning, MySpace, Tumblr, Whatsapp, Snapchat, Instagram and Pinterest for example – that do similar things for different audiences.

All these sites can link to each other and can include videos and photos.

Twitter: This is known as a micro-blogging site where users follow people or organisations that interest them and are followed in turn. On twitter users post short 140 character messages (tweets) to their followers but can also send private messages. You can also include links to pictures and other sites in a similar way to Facebook.

Flickr: This is a website for sharing photos where users can upload and share pictures. You can also search for photos

YouTube and Vimeo: These are websites for sharing videos and are organised in a similar way to Flickr. You can add comments to videos (and others can comment on your work).

Discussions and forums: Many websites have discussion boards and forums for debate and comment – these are particularly popular for news based sites

What we are talking about

The main emphasis of this document is to do with Facebook and Twitter – however this advice applies to any tool where you may put information, comment or opinion.

THE KEY THINGS YOU MUST DO TO PROTECT YOURSELF ONLINE

There are a few simple things you can think about and do to protect yourself and your posts

- You are an employee of the Diocese of Chester and social media blurs the distinction between the professional and private life of any individual. It is easy to think that you can have an element of privacy online. You can't. You can protect yourself by remembering at all times you are a public figure.
- Think about your friends and followers. You need to think about who you accept as friends on Facebook (and to a certain extent followers on twitter). Reaching out to a wide network of people who may share different views and express them in colourful ways may have many benefits. But you may need to think through the challenges of reaching a diverse group of people online and how you disassociate yourself from those who may cause you embarrassment. Similarly your friends may not appreciate your public position and post messages, photos or videos that could be very harmful. You could also be "tagged" in these photos bringing more attention. One example is the many incidents of teachers' careers getting into trouble because of the embarrassing holiday or night out picture. Some people consider having a professional and personal online persona. This can manage some of the risk but shouldn't be seen as the ultimate solution.
- Anything you say is in the public domain. You may think you are speaking to a controlled private group of friends but anything you put online can be regarded as published. Even if you put safeguards around whom you accept as friends or followers information can still be passed on.
- Legally posts may be subject to action under the laws of libel and defamation and online activity also has implications for Data Protection and copyright law. You cannot necessarily protect yourself by being anonymous or using a pseudonym. Legal cases have forced anonymous posters to reveal their identity.
- Clergy have found themselves the centre of unfavourable media attention after they posted social media comments. Most notably The Bishop of Willesden was suspended for comments about the Royal Wedding. A clergyman in the north criticised aspects of worship

and was widely criticised and rebuked. Your comments may not reach the same level of harm but if you criticise an aspect of your local church, parishioners or simply sound off at the end of a stressful day your comments could be taken and used against you. It may be regarded as a disciplinary matter if you make any derogatory comments about others on any social media site. You can protect yourself by only putting comments that you would also make in a public meeting; in your parish magazine or in local media.

- Anything you say is permanent. You may be able to delete a comment or entry made in haste but records could still have been seen. Your comment could have been reposted or copied to other sites. Even if you sent a direct message or personal email the recipient could find a variety of ways to keep a valid record of the comment. People could take a screen dump to save information that you may have thought is deleted.
- Your opinion matters. Everyone has an opinion and it is good and important to have debate. Freedom of speech is important and the church has a duty to hold a mirror up against society and society's values. Many do this through a blog (online diary). This is fine provided that you make clear the source of the opinion. It seems a bit of a modern cliché but you do need to state that views expressed are your own views and not necessarily that of your local or the national church. Many people put that statement on their twitter feed.
- Pictures tell a thousand words. Be careful about any pictures or videos you post. They may seem innocuous and fun to you but many people have fallen foul with the image of an unguarded moment. You may be "tagged" by a friend in photos that you don't wish to be seen in. You need to make sure they are removed.
- Don't forget copyright. It's easy to use Google to search and find that relevant image as a background to a blog entry or post. But beware that many images are protected by copyright and some organisations will pursue infringements. Similarly you need to be sure of the copyright of any music or film you wish to use.
- Online safeguarding is of essential importance. You need to be very aware of making sure you are safe, public and open in your communication with people – particularly the vulnerable. You need to have regard to our diocesan policies and the law. You should think very carefully about accepting "friend requests" from young or vulnerable people and in no circumstance should initiate a request with a vulnerable person. In any communications you should not attempt to send a direct message to a vulnerable person - all communication online should be open and transparent.
- Similarly you need to respect other people's confidentiality. It is easy to share someone else's story as an illustration of a point you wish to make. But you may not have that right (even if you change details). Make sure you are not the source of confidential information leaking out.
- Think about your personal details You need to keep yourself safe and not publish any personal or contact details – particularly addresses or phone numbers unless you are happy for people to know them.
- The single biggest thing you can do to protect yourself online is to assume anything you put is in the public domain and will be shared. If you do that and self edit your comments you are approaching the medium in a clear, responsible manner.

Who to contact for advice and support

Stephen Freeman