St Francis Xavier Catholic Primary

Social Media Policy

APPROVED BY: SENIOR LEADERSHIP

DATE APPROVED: NOVEMBER 2023

DATE REVIEWED:

DATE OF NEXT REVIEW: NOVEMBER 2026

1. Introduction

Social media is a useful tool for communications. It is an effective means to encourage participation, engagement and sharing. Every public body, including education establishments do need to consider its use as a positive resource. However, it very easy for it to be misused or to be used as a tool to attack others particularly with the post now - think later culture. There is also an increasingly blurred line between professional and personal relationships. This policy aims to give guidance on how to safeguard the school, staff, as well as the children and the school community.

Key points are:

- All users should be aware that posts are not private and are considered in the public domain
- All users should always remember that online participation results in the comments being permanently available and open to being republished in other media.
- All users should make sure that they stay within the legal framework and be aware that libel, defamation, copyright and data protection laws apply.

2. Using social media as a communication tool

The school takes in to consideration the following before using social media to communicate:

- Who is responsible for monitoring content and posting?
- Ensure the school owns the social media site and access is linked to one or two individual members of staff and passwords are known by only these members of staff.
- Establish terms of use on posting information for staff, pupils and parents.
- It is to be used for school information purposes only and to not be misunderstood and used as a complaints service.
- Prohibit unacceptable postings (defamatory, discriminatory, offensive, threatening, harassing or in breach of copyright, Intellectual Property (IP) or confidence).
- Allows the school to remove posts at its discretion and block members.
- Ensure comments are monitored and issues are dealt with quickly. Please be aware that the busiest time for students and parents to post would be in an evening therefore the staff allocated to monitor the profile should be given adequate time preferably in the mornings.
- ICT – Acceptable Use policy for both staff and pupils to be put in place.
- Ensure compliance with data protection – do not publish photos of children unless you have the signed consent of their parent.
- Make sure the ‘tagging function’ is enabled on the site, this will ensure children can’t tag anybody in the photographs uploaded, unless they have been approved by the members of staff who monitor the site.

3. Social Media – Basic Legal Issues

3.1 Copyright

- Copyright arises automatically in any original written or artistic work – there is no test of quality. It arises with posts, tweets, profiles, blogs and photos.
- Copyright in works created by an employee in the course of their duties belong to an employer.
- Copyright in works created by a student are owned by the student unless assigned to the school.
- If copyright is infringed and the post was made by an employee in the course of employment, the employer may be liable.
- Each social media site has clear terms and conditions about what is published usually making it clear that by publishing a free license is given for it to be reproduced and made available to the rest of the world by anyone.

3.2 Law with regard to inappropriate posts

Civil offences

Defamation:

A false statement must be made negligently and publically resulting in damage.

It is considered that public bodies cannot bring defamation actions though individuals can (whether a public body can support their employee in doing this with financial backing is also questionable).

It is an expensive process in money and time and prevention is the best way – getting the comments removed by the individual or the Internet service provider (ISP).

Protection from Harassment Act 1997:

This provides a civil offence of harassment allowing an individual to obtain an injunction to stop harassment and to obtain damages as appropriate. Harassment is defined as a course of conduct (of at least 2 occasions) causing the victim alarm or distress.

Criminal offences

Malicious Communications Act 1998: This relates to a post that is 'grossly offensive'.

Recent Criminal Prosecution Service (CPS) guidance provides limited circumstances when they will consider prosecuting for a malicious communication, including where it amounts to credible threats of violence to the person or damage to property or harassment under the 1997 Act.

Protection from Harassment Act 1997: This act also provides for a criminal offence in addition to the civil offence mentioned above.

Sexual Offences Act 2003: This Act is often used by the police relating to grooming and other actions with children on social media.

4. Social media usage in recruitment

Social media is increasingly used to check candidates' before offering a job.

It is important that the recruitment process and paper trail shows that appropriate decisions were made.

For further information on safer recruitment please see the link below:

http://www.education.gov.uk/aboutdfe/statutory/g00213145/safeguarding-children-safer-recruitment

Further advice can be obtained from Advanced HR

5. Governors

Even though Governors are volunteers and unpaid they still have a high degree of responsibility.

In particular:

- Governors should not disclose information, make commitments or engage in activities on behalf of the school, unless they are authorised to do so. This authority may already be delegated or may be explicitly granted depending on their role.
- Governors should not use social networking sites irresponsibly and ensure that neither their personal/professional reputation nor the school's reputation is compromised by inappropriate postings.

Any such postings could lead to either suspension or removal from the Governing Body.

All Governors are expected to sign up to the Governors Code of Conduct on appointment.

All Governors should consider the following;

- Consider carefully what you post on your online profile so that you do not compromise your professional position.
- Ensure that privacy settings are set correctly on the highest security level.
- Do not under any circumstances accept friend requests from a person you believe to be either a parent or a pupil at the school, where you are currently a Governor/or have previously been a Governor.
- Consider carefully before giving access to colleagues – are they really 'friends'?
- Do not make disparaging remarks about the school/colleagues/pupils or any member of the education community. Doing this in the presence of others may be deemed as bullying and/or harassment.
- Other users could post a photo on their profile where you could be named, so think about any photos you appear in. On Facebook, there is a tagging function you can enable onto your profile, which means everything you are tagged in i.e. pictures, comments, and statuses allows you to accept the content before it appears on your online profile and before it is connected to your name. If you do find inappropriate references to you and/or images of you posted by a 'friend' online you should contact them and the site to have the material removed.
- Parents and pupils may access your online profile and could, if they find the information or images offensive, complain to the school.
- Do not publish your date of birth and home address on any online profile. Identity theft is a crime on the rise with criminals using such information to access your bank or credit card account.
- Be aware of what monitoring, if any, maybe carried out by the education establishment.
- Ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation.

6. Senior Leadership

It is important that the school introduce social media policy at induction to their employees particularly with regard to the following:

- The school can be liable for the harassment of employees by other employees if this occurs in the course of employment. Employees are often online 'friends' with their colleagues. If concerning behaviour is happening online it may be happening in the workplace – don't ignore issues.
- All staff should be aware of their personal use of social media.
  - Staff are reminded of boundaries and are adhere to the responsibilities contained within the Staff Code of Conduct Policy.
- The school encourages the positive use of social networking sites as part of the educational process, clear guidance is given in ICT – acceptable use policy on what is considered to be appropriate contact with students.
- All must understand that social network sites are not private and are not considered outside the work domain.
- There is a significant risk of damage to the reputation of the school and teacher and damage to careers when inappropriate content is inputted online.
- All Staff should be aware of the role of the LADO (Local Authority Designated Officer for Safeguarding).
- The school can take action (including dismissal) for inappropriate online conduct outside working time provided:
  - There is actual or potential damage to the school's reputation.
  - There is evidence of harassment/bullying. Discrimination or otherwise offensive behaviour.
  - There is a clear policy making it clear what is acceptable and unacceptable; and
  - The school will respond in a reasonable and proportionate way.
- The school will seek advice from the HR Provider when considering disciplinary action.

7. Staff will:

- Consider carefully what you post on your online profile so that you do not compromise your professional position.
- Ensure that your privacy settings are set correctly on the highest security level.
- Do not under any circumstances accept friend requests from a person you believe to be either a parent or a pupil at your education establishment, where you are currently employed/or have previously been employed at.
- Consider carefully before giving access to colleagues – are they really
- 'friends'?
- Do not make disparaging remarks about your school/pupils or any member of the education community. Doing this in the presence of others may be deemed as bullying and/or harassment.
- Other users could post a photo on their profile where you could be named, so think about any photos you appear in. On Facebook, there is a tagging function you can enable onto your profile, which means everything you are tagged in i.e. pictures, comments, status' the function allows you to accept the content before it appears on your online profile and before it is connected to your name. If you do find inappropriate references to you and/or images of you posted by a 'friend' online you should contact them and the site to have the material removed.
- It is recommended that members of staff do not to use their first name and surname on social media sites.
- Parents and pupils may access your online profile and could, if they find the information or images offensive, complain to your education establishment.

- Do not publish your date of birth and home address on any online profile. Identity theft is a crime on the rise with criminals using such information to access your bank or credit card account.
- Be aware of what monitoring, if any, maybe carried out by the school
- Ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation.
- Make sure the GPS/ check-in facilities are disabled on the social networks you use.

8. Pupils

Internet and technologies are a part of everyday life for our children and young people; and as we can't be with them to watch their every click, it is imperative that safeguarding and education in this area is embedded thoroughly. This guidance should be introduced to pupils at the beginning of each year.

- It should be made clear to pupils that having an online profile is against all rules and regulations in place if you access or create an account under the age of 13. This applies to Facebook, Twitter, Instagram, Snapchat and You Tube.
- When accessing these accounts despite the rules in place pupils need to be aware of the amount of personal information they can potentially give away. General guidance around what is safe and what isn't should be talked about in the school. For example an interest is ok; naming the school they attend is giving away too much information.
- Pupils should be encouraged not to put pictures of them online but to use avatars or a picture of an interest e.g. a football. Pupils can give away information in images they upload especially in school uniforms or any other uniform indicating a club they attend.
- Education around putting privacy settings on is imperative.
- Pupils should be made aware of the dangers GPS/ check-in facilities can potentially put them in. GPS and check in facilities allow pupils to geographically locate themselves in a status. It can also identify their address and/or whether they are on holiday. If pupils were to use it when they are out visiting/eating with friends they could also be putting each other in danger. It is also advised that pupils do not check-in at school as this locates and posts what school they go to. GPS/check-in can come become automatic when it is enabled on smartphones.
- Pupils should be encouraged to be wary about publishing specific and detailed private thoughts online.
- Pupils are taught to consider their digital footprint.
- eSafety advice, updates and information should be given to pupils on a regular and meaningful basis.
- Pupils should be made aware of how they can seek help and advice when problems online do occur, it is advised that the CEOP (Child Exploitation and Online Protection Centre) button is talked about in the education establishment and ideally embedded onto the education establishment website so that pupils are aware of where to go to if they needed to use it.
- Pupils need to be made aware of legislation which could affect what they put/do online
- Parents should be contacted if it is highlighted that a child is accessing a site that is deemed to be inappropriate or not age appropriate.
- All new pupils need to be made aware of the rules and regulations around eSafety.

- All Students need to be made aware of whom the Designated Safeguarding Lead is in the school to discuss any concerns or worries.

9. Inappropriate online behaviour by parents/pupils/Governors

Online conduct by parents, pupils and Governors can have a devastating impact on individual teachers/staff and the school. It has the potential to lead to stress related illness and absence from work. The education establishment should support any staff member when it becomes aware of any concerns. All employers have a duty of care to protect the health and safety of staff in the course of employment.

Key points:

- Ensure staff are aware they should let the Head of School know of any concerns.
- Consider initially speaking to the child/parent/Governor and requesting they remove the post.
- Consider if criminal offences may have occurred and speak to your local police officer (see guidance in section 7 on legal issues).
- Report your concern to the host of the site in writing and ask that they remove the post.
- Most social media sites do have a report abuse button.

Parents Photography

Concern remains over parents photographing their children at school events.

- The Information Commissioner, who is responsible for overseeing data protection, has made it clear that images taken by parents for personal or recreational purposes such as with mobile phone, digital camera or camcorder are exempt from the Data Protection Act.
- However, the school may still have restrictions when taking photographs or video or other images for child protection reasons or to prevent disturbances or because of concerns that parents have been using photos inappropriately.
- It is appropriate to remind parents in writing and/or at the event that the photographs should only be for personal use and must not be posted on social media sites if they include other children. The school may also consider it appropriate to restrict photographs to the end of the event so that particular children can be removed from the photographs.
- There are a number of issues to consider with regard to this and the solution will be different for each event. The approach will depend on the particular issues and past concerns.

Appendix 1
Guidance on Using Facebook Responsibly

Our education establishment is committed to promoting the safe and responsible use of the Internet and student's access to social media sites can be a concern. Whilst children cannot access Facebook or other social networking sites at the education establishment, they could have access to it on any other computer or mobile technology. Websites such as Facebook offer good communication and social connections, however they are created with their audience in mind and this is specifically 13 years old. Possible risks for children under 13 using the site may include:

- Facebook use 'age targeted' advertising and therefore your child could be exposed to adverts of a sexual or other inappropriate nature, depending on the age they stated they were when they registered.
- Children may accept 'friend requests' from people they don't know in real life which could increase the risk of inappropriate contact or behaviour (grooming).
- Language, games, groups and content posted or shared on Facebook is not moderated, and therefore can be offensive, illegal or unsuitable for children.
- Photographs shared by users are not moderated and therefore children could be exposed to inappropriate images or even post their own.
- Underage users might be less likely to keep their identities private and lying about their age can expose them to further risks regarding privacy settings and other options.
- Facebook could be exploited by bullies and for other inappropriate contact.
- Facebook cannot and does not verify its members therefore it is important to remember that if your child can lie about who they are online, so can anyone else.

We feel that it is important to point out to parents/carers the risks of underage use of such sites, so you can make an informed decision as to whether to allow your child to have a profile or not. These profiles will have been created away from the education establishment and sometimes by a child, their friends, siblings or even parents. We will take action (such as reporting aged profiles) if a problem comes to our attention that involves the safety or wellbeing of any of our children. Should you decide to allow your children to have a Facebook profile we strongly advise you to do the following:

- Check their profile is set to private and that only 'friends' can see information that is posted;
- Make sure they have privacy settings on to a high standard so they have to accept 'tags' in posts and pictures.
- Remove the location setting on statuses, this can pin point to their friends exactly what road they're stood on when writing something on Facebook.
- Monitor your child's use and talk to them about safe and appropriate online behaviour such as not sharing personal information and not posting offensive messages or photos;
- Ask them to install the CEOP (Child Exploitation and Online Protection Centre) application from www.facebook.com/clickceop on their profile. This places a bookmark on their profile to CEOP and the 'Report Abuse' button which has been known to deter offenders;

- Have a look at the advice for parents/carers from Facebook www.facebook.com/help/?safety=parents
- Set up your own profile so you understand how the site works and ask them to add you as a friend on their profile so you can keep track of what they are posting online;
- Make sure your child understands the following rules:

  - Always keep your profile private;
  - Never accept friends you don't know in real life;
  - Never post anything which could reveal your identity;
  - Never post anything you wouldn't want your parents to see;
  - Never agree to meet someone you only know online without telling a trusted adult;
  - Always tell someone if you feel threatened or someone upsets you.

We recommend that all parents/carers visit the CEOP ThinkuKnow website for more information on keeping your child safe online or to report online abuse please see link below:

http://ceop.police.uk/safety-centre/

Appendix 2
Guidance on using Apps - Staff

Staff who use Apps (for example WhatsApp/Facebook Messenger) for school purposes on their own device must agree to these terms of use.

Deliberate and negligent misuse of the software and actions against the terms of use set out may result in disciplinary action.

- Apps (for example WhatsApp/Facebook Messenger) can be appropriately used for school business use.
- All information recorded in these Apps is subject to requests made by the public under the Freedom of Information Act 2000 and Data Protection Act 2018, therefore if information which is necessary for the school to fulfil its duties under these legislations is held in these channels, staff will be required to provide their device to enable the school's ICT Team to access this.
- Staff are reminded that erasing, destroying or concealing information with the intention of preventing its disclosure, following receipt of a request, is a criminal offence under section 77 of the Freedom of Information Act 2000. This offence can apply to both a public authority (the school) and to any person who is employed by or is subject to the direction of the school.
- If groups are created, admins should regularly monitor group members to ensure only those who still require access to the group are included.
- If the device is lost or stolen, employees must report this to the school immediately who are required to register it as a security incident and potential data protection breach.
- Staff must always ensure the security of the device by using a PIN, password, or key-lock if available.

Appendix 3
Guidance on Creating Social Media Sites on Behalf of the school

A.1 CREATION OF SITES

A.1.1 Staff members participating in social media for work purposes are expected to demonstrate the same high standards of behaviour as when using other media or giving public presentations on behalf of the school.

A.1.2 Prior to creating a site, careful consideration must be given to the purposes for using social media and whether the overall investment is likely to be worthwhile for achieving the proposed pedagogical outcome.

A.1.3 The proposed audience and level of interactive engagement with the site, for example whether pupils, staff or members of the public will be able to contribute content to the site, must be discussed with the Head of School.

A.1.4 Staff members must consider how much time and effort they are willing to commit to the proposed site. They should be aware that maintaining a site is not a one-off task, but involves a considerable time commitment.

A.1.5 The Head of School must take overall responsibility to ensure that enough resources are provided to keep the site refreshed and relevant. It is important that enough staff members are trained and are able to maintain and moderate a site in case of staff absences or turnover.

A.1.6 There must be a careful exit strategy and a clear plan from the outset about how long the site will last. It must not be neglected, creating a potential risk to the education establishment's brand and image.

A.1.7 Consideration must also be given to how the success of the site will be evaluated to assess whether the site has achieved the proposed objectives.

A.2 CHILDREN AND YOUNG PEOPLE

A.2.1 When creating social media sites for children and young people and communicating with them using such sites, staff members must at all times be conscious of their responsibilities; staff must always act in the best interests of children and young people.

A.2.2 When creating sites for children and young people, staff members must be alert to the risks to which young people can be exposed. Young people's technical knowledge may far exceed their social skills and awareness – they may post sensitive personal information about themselves, treat online 'friends' as real friends, be targets for 'grooming' or become victims of cyberbullying.

A.2.3 If children and young people disclose information or display behaviour or are exposed to information or behaviour on these sites that raises safeguarding or other concerns, appropriate authorities must be informed immediately. Failure to do so could expose vulnerable young people to risk of harm.

A.2.4 Staff members must also ensure that the webspace they create on third party sites comply with the site owner's minimum age requirements (this is often set at 13 years). Staff members must also consider the ramifications and possibilities of children under the minimum age gaining access to the site.

A.2.5 Care must be taken to ensure that content is suitable for the target age group and contributors or 'friends' to the site are vetted.

A.2.6 Careful thought must be given to the profile of young people when considering creating sites for them. For example, the internet may not be the best medium to communicate with vulnerable young people (or indeed any age group) receiving confidential and sensitive services from the school. It may not be possible to maintain confidentiality, particularly on third-party-hosted sites such as social networking sites, where privacy settings may not be strong enough to prevent breaches of confidentiality, however inadvertent. If in doubt, you must seek advice from the Head of School.

A.3 APPROVAL FOR CREATION OF OR PARTICIPATION IN WEBSPACE

A.3.1 The school's social media sites can be created only by or on behalf of the school. Site administrators and moderators must be employees or other authorised people.

A.3.2 Approval for creation of sites for work purposes, whether hosted by the education establishment or hosted by a third party such as a social networking site, must be obtained from the Head of School.

A.3.3 Approval for participating, on behalf of school, on sites created by third parties must be obtained from the Head of School.

A.3.4 Content contributed to own or third-party hosted sites must be discussed with and approved by the Head of School

A.3.5 The Head of School must be consulted about the purpose of the proposed site and its content. In addition, the Head of School's approval must be obtained for the use of the education establishment logo and brand.

A.3.6 Be aware that the content or site may attract media attention. All media enquiries must be forwarded to the Head of School immediately. Staff members must not communicate with the media without the advice or approval of the Executive Headteacher.

A.4 CONTENT OF WEBSPACE

A.4.1 The school's hosted sites must have clearly expressed and publicised policies. Third-party hosted sites used for work purposes must have policies that conform to the education establishment or Council standards of professional conduct and service.

A.4.2 Staff members must not disclose information, make commitments or engage in activities on behalf of the school without authorisation.

A.4.3 Information provided must be worthwhile and accurate; remember what is published on the site will reflect on the school's image, reputation and services.

A.4.4 Stay within the law and be aware that child protection, privacy, data protection, libel, defamation, harassment and copyright law may apply to the content of social media.

A.4.5 Staff members must respect their audience and be sensitive in the tone of language used and when discussing topics that others may find controversial or objectionable.

A.4.6 Permission must be sought from the relevant people before citing or referencing their work or referencing service providers, partners or other agencies.

A.4.7 The schools hosted sites must always include the school's logo or brand to ensure transparency and confidence in the site. The logo should, where possible, link back to the relevant page on the education establishment website.

A.4.8 Staff members participating in the school's hosted or other approved sites must identify who they are. They must disclose their positions within the education establishment on these sites.

A.4.9 Staff members must never give out their personal information such as home contact details or home email addresses on these sites.

A.4.10 Personal opinions should not be expressed on official sites.

A.5 CONTRIBUTORS AND MODERATION OF CONTENT

A.5.1 Careful consideration must be given to the level of engagement of contributors – for example whether users will be able to add their own text or comments or upload images.

A.5.2 Sites created for and contributed to by pupils must have the strongest privacy settings to prevent breaches of confidentiality. Pupils and other participants in sites must not be able to be identified.

A.5.3 The content and postings in the school's hosted sites must be moderated. Moderation is the responsibility of the team that sets up or initiates the site.

A.5.4 The team must designate at least two approved Administrators whose role it is to review and moderate the content, including not posting or removal of comments which breach the schools policies. It is important that there are enough approved moderators to provide cover during leave and absences so that the site continues to be moderated.

A.5.5 For third-party-hosted sites such as social networking sites used for work purposes, the responsibility for protection and intervention lies first with the host site itself. However, different sites may have different models of intervention and it is ultimately the responsibility of the staff member creating the site to plan for and implement additional intervention, for example in the case of content raising child safeguarding concerns or comments likely to cause offence.

A.5.6 Behaviour likely to cause extreme offence, for example racist or homophobic insults, or likely to put a young person or adult at risk of harm must never be tolerated. Such comments must never be posted or removed immediately and appropriate authorities, for example the Police or Child Exploitation and Online Protection Centre (CEOP), informed in the case of illegal content or behaviour.

A.5.7 Individuals wishing to be 'friends' on a site must be checked carefully before they are approved. Their comments must be reviewed regularly and any that do not comply with the social network guidance must not be posted or removed. **The school will not allow any outsiders to become friends of the site and the site is limited to known people only, in the case of adults, those who have undergone appropriate security checks.**

A.5.8 Any proposal to use social media to advertise for contributors to sites must be approved by the Head of School.

A.5.9 Approval must also be obtained from the Head of School to make an external organisation a ‘friend’ of th