Beamish and Pelton Federation

Social Media/ Networking Policy

September 2020

All staff employed at Beamish and Pelton Federation are subject to this policy

1. Introduction

Social media is a broad term for any kind of online platform which enables people to directly interact with each other. It allows people to share information, ideas and views. Examples of social media include blogs, Facebook, LinkedIn, Twitter, Google+, Instagram, Myspace and YouTube. Social networking/media is an innovative and efficient way of connecting and engaging with customers and communities of interest at a low cost and should an employee be required to access or participate in such sites for work purposes, they must adhere to the School's Social Networking Policy, Procedure and Guidance.

The widespread availability and use of social networking applications bring opportunities to understand, engage and communicate with our audiences in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, while employees are encouraged to engage, collaborate and innovate through social media, they should also be aware that there are some associated risks, especially around issues of safeguarding, bullying and personal reputation.

The use of social networking sites introduces a range of potential safeguarding risks to children and young people.

Potential risks can include, but are not limited to:

- online bullying
- grooming, exploitation or stalking
- exposure to inappropriate material or hateful language
- encouraging violent behaviour, self-harm or risk taking

Our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults. The policy requirements in this document aim to provide this balance to support innovation and Schools of the 21st Century, whilst providing a framework of good practice. They apply to all members as defined by School representatives.

2. Purpose

The purpose of this policy is to provide a framework that will enable school representatives to enjoy the benefits of social networking while understanding the standards of conduct expected by the Federation. It is intended to minimise the risks that can impact on the wellbeing of staff, pupils and the reputation of the Federation of Beamish and Pelton Primary schools.

Our key purposes are to ensure:

- ✓ all children are safeguarded
- ✓ that Beamish and Pelton Federation, its leaders and governors are not exposed to legal risks
- ✓ that the reputation of Beamish and Pelton Federation, staff and governors at the school are not adversely affected

- ✓ that any users are able to clearly distinguish where information provided via social networking applications is legitimately representative of Beamish and Pelton Federation

3. Scope

This policy covers the use of social networking applications by School Employees, Governors and/or Elected Members and by partners or other third parties on behalf of the School. These groups are referred to collectively as 'School representatives' for the purpose of this policy. The requirements of this policy apply to all uses of social networking applications which are used for any school or local authority related purpose and regardless of whether the applications are hosted corporately or not. They must also be considered where School representatives are contributing in an official capacity to social networking applications provided by external organisations.

Social networking applications include, but are not limited to:
Blogs, Online discussion forums, collaborative spaces, media sharing services, 'Microblogging' applications. Examples include Twitter, Facebook, Instagram, Snapchat, Whatsapp and You Tube. Many of the principles of this policy also apply to other types of online presence such as virtual worlds.

4. Guidance/protection for staff on using social networking in school

All School representatives should bear in mind that information they share through social networking applications, even if they are on private spaces or using personal devices, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the School and Local Authority Equality and Safeguarding Policies.
School staff will not invite, accept or engage in communications with parents or children from the school community to any personal social networking sites while in employment across the Federation of Beamish and Pelton Primary Schools.

With regard to personal safeguarding, you should report any harassment or abuse you receive online while using your work accounts. Any communication received from children to School Representatives must be immediately reported to the Head Teacher – Designated Child Protection Officer and procedures for safeguarding followed.

If a School Representative is made aware of any other inappropriate communications involving any child and social networking. These must be reported immediately as above. The Online Safety policy must be used at all times when children use ICT and access the internet in school.

Use of Social networking sites in worktime

Use of social networking applications in work time for personal use only is not permitted, unless permission has been given by the Head teacher.

Social Networking as part of School Service

All proposals for using social networking applications as part of a school service (whether they are hosted by the school or by a third party) must be approved by the Head teacher first.

The following are not considered acceptable at Beamish and Pelton Federation of Schools:

- ✓ The use of the schools name, logo, or any other published material without written prior permission from the Headteacher. This applies to any published material including the internet or written documentation.
- ✓ The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.
- ✓ The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.
- ✓ The posting of any images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities without consent and GDPR compliance (see policy).

In addition to the above everyone at Beamish and Pelton Federation must ensure that they:

- ✓ Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school.
- ✓ Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.

School staff will not invite, accept or engage in communications with parents or children from the school community to any personal social networking sites while in employment at Beamish and Pelton Federation.
Any communication received from children to School Representatives must be immediately reported to the Head Teacher, designated Child Protection Officer and procedures for safeguarding followed.

- Staff members who use the school Twitter accounts must sign an AUP.
- No social media apps are to be installed on school Ipads apart from the following two exceptions:
  Twitter can be installed on staff Ipads at Pelton Primary School only by staff who are responsible for running the school's Twitter account.
  Facebook can only be installed on staff Ipads at Beamish Primary School only by staff who are responsible for running the school's Facebook account.
- No member of staff should interact with any pupil in the school on social networking sites
- No member of staff should interact with any ex-pupil in the school on social networking sites who is under the age of 18
- This means that no member of the school staff should request access to a pupil's area on the social networking site. Neither should they permit the pupil access to the staff members' area e.g. by accepting them as a friend.
- Where family and friends have pupils in school and there are legitimate family links, please inform the head teacher. However, it would not be appropriate to network during the working day on school equipment
- It is illegal for an adult to network, giving their age and status as a child
  If you have any evidence of pupils or adults using social networking sites in the working day, please contact the named Child Protection person in school

5. Guidance/protection for staff on using social networking outside of school/for personal use

Employees should think carefully about posting information and below is general guidance for employees to consider:

- That the personal image an employee projects in social media may adversely reflect on the image of the Federation.

- Decide whether to identify themselves as an employee of the School. This could be for example, by listing their employer's name or nature of business in an appropriate section. If this link is made, then an employee must consider that anything they participate in or upload can be connected with the Federation.

- When talking about their school, an employee should make it clear that their views are their own and not that of the Federation. This is particularly important if the employee could be viewed as being in a position of responsibility within the Federation. For example, if the employee's role is a high profile one, the messages posted could be construed as an official statement.

- Be mindful of their association with Beamish and Pelton Community Primary Schools and Durham County Council in online spaces. If an employee identifies themselves as an employee, they must ensure that their profile and related content is consistent with how they wish to present themselves professionally with colleagues, parents and families.

- If an employee does not intentionally identify themselves as working for the School they need to be mindful that their comments, videos and photographs could identify a link with the School. For example, a picture posted on a site which has the employee in their uniform or a negative comment about their work which can be traced back to the School. Any online name and other titles should also not include any reference to the School.

- Be aware that they are personally responsible for any content they post or write online and that this can result in the information being permanently available and therefore it is open to be republished in other media in the public domain.

- Do not publicise any colleagues or children's personal or confidential information, such as contact details or photographs.

- Understand their own online privacy settings. Settings must be checked and employees should be clear who can see their information. It is the responsibility of the staff member to ensure their social media accounts are private and personal information kept confidential.

- Hacking has become a problem for some social media sites, so employees should be aware that their account may be vulnerable to hacking. If an account is hacked, an employee should report any incident to the site and keep a record of the bogus

information posted on the account.

- Only access a social networking site for personal use using School equipment in their own time.

- Employees should be aware that in line with the Acceptable Usage Policy and the Data Protection policy managers can check on internet use if they suspect that any employee is abusing access for personal use.

- Understand and adhere to the Federation's Acceptable Usage Policy, Online Safety Policy and Code of Practice and the Equality and Diversity Policy.

Any communications or content you publish that causes damage to the School, Local Authority, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the School and Local Authority Dismissal and Disciplinary Policies apply. Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.

Local Authority expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

6. Guidance/protection for Pupils on using social networking

- No pupil under 13 should be accessing social networking sites. This is the guidance from Facebook, Instagram and Snapchat.
- No children under 16 should be accessing social media platforms such as TikTok and Whatsapp.
- No pupil may access social networking sites during the school working day. YouTube is blocked for children in school and only available for staff.
- All mobile phones must be handed into the KS2 office or to the classroom teacher at the beginning of the school day and must be switched off. Failure to follow this guidance will result in a total ban for the student using a mobile phone.
- No pupil should attempt to join a staff member's areas on networking sites. If pupils attempt to do this, the member of staff is to inform the Head teacher. Parents will be informed if this happens.
- No school computers are to be used to access social networking sites at any time of day.
- Any attempts to breach firewalls will be logged on the school's SmoothWall filtering system and the Mrs Stavers and Mrs Short (safeguarding leads) will be instantly notified. If breaches are regular from a pupil, this will result in a ban from using school ICT equipment other than with close supervision.
- Please report any improper contact or cyber bullying to the class teacher in confidence as soon as it happens.

- We have a zero tolerance to cyber bullying. Any incidences of cyberbullying will be logged on CPOMs and the designated safeguarding team and parents will be informed.

If a School Representative is made aware of any other inappropriate communications involving any child and social networking. These must be reported immediately as above. The Online Safety policy must be used at all times when children use ICT and access the internet in school.

7. Enforcement and reporting concerns

Any breach of the terms set out below could result in the application or offending content being removed in accordance with the published complaints procedure and the publishing rights of the responsible School representative being suspended.

The Local Authority reserves the right to require the closure of any applications or removal of content published by School representatives which may adversely affect the reputation of the School or put it at risk of legal action.

Any content or online activity which raises a safeguarding concern must be reported to the lead safeguarding officer in the Federation.
Any online concerns should be reported as soon as identified as urgent steps may need to be taken to support the child.
With regard to personal safeguarding, you should report any harassment or abuse you receive online while using your work accounts.

Child protection guidance

If the head teacher receives a disclosure that an adult employed by the school is using a social networking site in an inappropriate manner as detailed above they should:

- Record the disclosure in line with their child protection and safeguarding policy
- Schools must refer the matter to the Local Authority.
- If the disclosure has come from a parent, take normal steps to calm the parent and explain processes
- If disclosure comes from a member of staff, try to maintain confidentiality
- The Local Authority will advise whether the member of staff should be suspended pending investigation after contact with the police. It is not recommended that action is taken until advice has been given.
- If disclosure is from a child, follow your normal process in your child protection policy until the police investigation has been carried out

Cyber Bullying

By adopting the recommended no use of social networking sites on school premises, Beamish Primary and Pelton Community Primary School protects themselves from accusations of complicity in any cyber bullying through the provision of access.

- Staff should never engage with cyberbullying incidents. If in the course of your employment with this school/trust, you discover a website containing inaccurate,

inappropriate or inflammatory written material relating to you, or images of you which have been taken and/or which are being used without your permission, you should immediately report this to a senior manager at your school. Staff should keep any records of the abuse such as text, emails, voicemail, website or social media. If appropriate, screen prints of messages or web pages could be taken and the time, date and address of site should be recorded.

- Parents should be clearly aware of the Federation's Online Safety policy of access to social networking sites.

Where a disclosure of bullying is made, schools now have the duty to investigate and protect, even where the bullying originates outside the school. This can be a complex area, and these examples might help:

- A child is receiving taunts on Facebook and text from an ex pupil who moved three months ago: This is not a school responsibility, though the school might contact the new school to broker a resolution.
- A child is receiving taunts from peers. It is all at weekends using Instagram direct message and Facebook. The pupils are in the school: The school has a duty of care to investigate and work with the families, as they attend the school.
- A child is receiving taunts from peers. It is all at weekends using Facebook. The pupils are in Y5: The school has a duty of care to investigate and work with the families, as they attend the school. However, they are also fully within their rights to warn all the parents (including the victim) that they are condoning the use of Facebook outside the terms and conditions of the site and that they are expected to ensure that use of the site stops. At any further referral to the school the school could legitimately say that the victims and perpetrators had failed to follow the schools recommendation. They could then deal with residual bullying in the school, but refuse to deal with the social networking issues.

- Once disclosure is made, investigation will have to involve the families. This should be dealt with under the school's adopted anti bullying policy.
- If parent / carers refuse to engage and bullying continues, it can be referred to the police as harassment
- This guidance can also apply to text and mobile phone cyber bullying.

<u>Inappropriate personal use</u>

Outlined below are examples of conduct which may lead to disciplinary action being taken against an employee and in some cases could constitute gross misconduct. This list is not exhaustive and each case will be determined on the individual facts.

- If an employee identifies themselves as an employee, expressing any negative (for example, negative views regarding the Council, Officers/Members or their employment), defamatory (statements made that have or may cause harm to the Council's reputation) or unlawful comments on subjects that might not necessarily relate to a Council service, it could result in disciplinary action, e.g. making inappropriate comments about management and/or the Council's policies to friends on Facebook.

- If an employee does include a reference to their employment with the Council, for example listing their employer in their personal details on a social media website, they must ensure that all communication/videos/behaviour online does not breach the Council's Equality and Diversity Policy or damage the reputation of the Council. e.g. an employee's open profile page states that they are employed by the Council and they make comments and disparaging remarks about the community which they work with on their status updates.
- Do not use the Durham County Council logo or reproduce any other form of Council communication or documents, without express permission. Also avoid use of Council email addresses, which would provide a clear link to the Council.

- Where possible, employees should consider the appropriateness of accepting customers of the Council as 'friends' on social networking sites or 'following' potentially negative, defamatory or unlawful third party social media feeds. This could have an implication if the employee's profile as a County Council employee could be linked to these feeds. e.g. "liking" comments relating to extremist organisations.

- If an employee's work involves anyone who is a 'friend' or 'follower' on social media, the employee must notify their manager about the relationship. The manager will then be responsible for deciding whether it is appropriate for the employee to be involved with the "friend's" contact with the Council. This is to avoid any allegations of preferential treatment.

- Under no circumstances make offensive comments about, or to colleagues or customers on the internet. Harassment, cyber-bullying and/or discrimination will not be tolerated and would be deemed a disciplinary offence which may constitute gross misconduct.

- To not publish/disclose any rumours/internal and/or confidential information about the Council or related third parties, for example customers or suppliers etc.

- Ensure no comments or content could breach copyright or the Data Protection Act.

- Failure to follow these guidelines could result in disciplinary action being taken against an employee.

8. Monitoring and review

If the manager reasonably believes that an employee has breached this policy, from time to time the school will monitor or record communications that are sent or received from within the school/trust's network.

This policy will be reviewed on a yearly basis and, in accordance with the following, on an as-and-when-required basis:

- legislative changes
- good practice guidance
- case law
- significant incidents reported.

This policy does not form part of any employee's contract of employment and may also, after consultation with the trade unions, be amended from time to time by the Federation.

9. Legislation

Acceptable use of social networking must comply with UK law. In applying this policy, the Federation will adhere to its rights, responsibilities and duties in accordance with the following:

- Regulation of Investigatory Powers Act 2000
- General Data Protection Regulations (GDPR) 2018
- The Human Rights Act 1998
- The Equality Act 2010
- The Defamation Act 2013

10. Conclusion

The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media – the principles set out in this policy must be followed irrespective of the medium.

When using social media, staff should be aware of the potential impact on themselves and the employer, whether for work-related or personal use; whether during working hours or otherwise; or whether social media is accessed using the employer's equipment or using the employee's equipment.

11. Related Federation Documentation

- Online Safety policy
- Data Protection Policy
- Safeguarding and Child protection policy
- Staff Acceptable Use Policy
- Complaints procedure
- Equality policy
- Internet Policy in school