ICT010 – Social Media Policy

Title	ICT010 – Social Media Policy
Version	1.0
Date	September 2017
Author	ICT Coordinator / K Allison
Approved by headteacher	
Approved by governing body	
Next review date	September 2018

Modification History			
Version	**Date**	**Description**	**Revision Author**

Kell Bank CE Primary School

ICT010 – Social Media Policy

Introduction
Kell Bank CE Primary School recognises the importance of the Internet and mobile communications technology in shaping public and internal thinking about the school.

Rationale
The school recognises the value to our staff in joining in and helping shape educational direction through blogging and interaction in social media.

We are committed to supporting rights to interact knowledgeably and socially on the Internet through email, blogging and communication in social media.

We are also committed to ensuring that all staff employed by the school are aware of their vulnerability to identity theft and the potential threat to their profile and professional standing by posting inappropriate personal information on the internet via social networking sites thus leaving an "electronic footprint", compromising themselves and / or the school.

It's not just a matter of personal safety. What seems frivolous or even trivial to you in a friendship group could damage your reputation when seen by others. For example, pictures taken at parties and posted on a profile can cause embarrassment, or worse, when seen by parents, colleagues and employers. Before you post something, ask yourself what impression someone would get from seeing your web presence? Can this be linked back to my place of work and cause embarrassment or damage my professional role and /or Kell Bank CE Primary School.

Aims
The aims of this policy is to make clear to all staff the steps necessary to protect themselves and the school in making appropriate decisions about what content is suitable in blogs, personal & public websites, postings on wikis, video or picture sharing sites and when responding to comments from posts either publically or via email. The schools ICT security policy and e-safety Policy remains in effect.

N.B. Please note that this policy applies only to online content that has a direct or indirect connection or link to Kell Bank CE Primary School or that may be inferred as being the opinion of the school. The policy does not infringe upon your personal interaction or commentary online unless the contents of such interaction or commentary are seen as a breach of professional trust between you and our school.

Guidelines - Interaction on the Internet and via mobile communication technology

The Professional expectations of confidentiality regarding the day-to-day functions, practices and events that happen within Kell Bank CE Primary School do not change when using the Internet or mobile communication technology.

- Staff are expected to speak respectfully about the school and our current and potential employees, students, and partners.
- Do not engage in 'name calling 'or behaviour that will reflect negatively on the school's reputation. Note that the use of unfounded or derogatory statements or misrepresentation is not viewed favourably and may result in formal disciplinary action. Unless given permission by your manager, you are not authorised to speak on behalf of the School, nor to represent that you do so.
- Any online presence should not make reference to Kell Bank CE Primary School for example, you are not authorised to utilise your school email address when joining social networking sites or making the school supplied email address your primary method of contact.
- Kell Bank CE Primary School logo and name may not be used without explicit permission in writing from the Headteacher. This is to prevent the appearance that you speak for or represent the company officially.
- Recognise that staff are legally liable for anything they write or present online. Staff may be formally disciplined by the school for commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment. You may also become the subject of litigation by colleagues, and any individual or company that views your commentary, content, or images as defamatory, pornographic, proprietary, harassing, libelous or creating a hostile work environment.
- Honour the privacy rights of your colleagues by seeking their permission before writing about or displaying internal school events that might be considered to be a breach of their privacy and confidentiality and ensure that the school policy on displaying pupil images and information is adhered to.
- Recognise that as a member of staff of Kell Bank CE Primary School your online opinions, interactions and internet presence are influential to the young people that we support and as such should always be balanced and appropriate so that no inference of political, sexual or racist bias can be construed.

Summary

The above points are not exhaustive and only cover a range of what Kell Bank CE Primary School consider confidential and proprietary. If you have any questions about the appropriateness of online information released publicly or doubts of any kind, please speak to your line manager or a member of the senior leadership team before releasing information that could potentially harm our school, or our staff, students, and school community.

School representatives must adhere to the following Terms of Use. The Terms of Use below apply to all uses of social networking applications by all school representatives. This includes, but is not limited to, public facing applications such as open discussion forums and

internally-facing uses such as project blogs regardless of whether they are hosted on school network or not.
Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. The school 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. Social Networking applications:

- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns
- Must not be used in an abusive or hateful manner
- Must not be used for actions that would put school representatives in breach of school codes of conduct or policies relating to staff.
- Must not breach the school's misconduct, equal opportunities or bullying and harassment policies
- Must not be used to discuss or advise any matters relating to school matters, staff, pupils or parents
- No staff member should have a pupil or former pupil under the age of 18 as a 'friend' to share information with
- Employees should not identify themselves as a representative of the school
- References should not be made to any staff member, pupil, parent or school activity / event unless prior permission has been obtained and agreed with the Head Teacher
- Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally effects the employer's reputation then the employer is entitled to take disciplinary action. Violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment.

Guidance/protection for staff on using social networking

- 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 in writing.
- 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 Guidance/protection for Pupils on using social networking
- No pupil under 13 should be accessing social networking sites. This is the guidance from both Facebook and MSN. There is a mechanism on Facebook where pupils can be reported via the Help screen; at the time of time of writing this policy the direct link for this is: http://www.facebook.com/help/contact.php?show_form=underage
- No pupil may access social networking sites during the school working day
- All mobile phones must be handed into the office at the beginning of the school day, the Internet capability 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 result in a ban from using school ICT equipment other than with close supervision
- Please report any improper contact or cyber bullying to you tutor / class teacher in confidence as soon as it happens.
- We have a zero tolerance to cyber bullying

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 policy
- Schools must refer the matter to the LA who will investigate via North Yorkshire Police Child Protection Team.
- 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 LA 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, Kell Bank CE Primary School protects themselves from accusations of complicity in any cyber bullying through the provision of access. Parents should be clearly aware of the school's 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 MSN 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: This is the tricky one. 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