Part of the Tibberton CE Primary School and
St Lawrence CE Primary School Federation

Social Media Policy

Revised: Autumn Term 2020

Consultation with staff and Governors

and adoption of policy: Autumn Term2020

Review date: Autumn Term 2021

Statement of Intent

Tibberton & St Lawrence CE Primary School's understands that social media is a growing part of life outside of school. We have a responsibility to safeguard our pupils against potential dangers when accessing the internet at school, and to educate our pupils about how to protect themselves online when outside of school.

1. Key Roles and Responsibilities

- 1.1 The Governing Board has overall responsibility for the implementation of the Social Media Policy and procedures at Tibberton & St Lawrence.
- 1.2 The Governing Board has responsibility for ensuring that the Social Media Policy, as written, does not discriminate on any grounds, including but not limited to: ethnicity/national origin, culture, religion, gender, disability or sexual orientation.
- 1.3 The Governing Board has responsibility for handling complaints regarding this policy as outlined in the school's Complaints Policy.
- 1.4 The Heads of School will be responsible for the day-to-day implementation and management of the Social Media Policy and procedures of Tibberton & St Lawrence.
- 1.5 Staff, including teachers, support staff and volunteers, will be responsible for following the Social Media Policy and for ensuring pupils do so also. They will also be responsible for ensuring the policy is implemented fairly and consistently in the classroom.
- 1.6 Parents and carers will be expected to take responsibility for the social media habits of their child/children at home.
- 1.7 Parents and carers will be expected to promote safe social media behaviour.

2. The School's E-safety Team and Network Manager

- 2.1 The school's e-safety team consists of: St Lawrence: Mr Laith A-Asmar and Mrs A Moore and Tibberton: Mrs North

3. Definitions

- 3.1 Tibberton & St Lawrence Primary School defines "social media" as any online platform that offers real-time interaction between the user and other individuals or groups including but not limited to:
    - Online discussion forums, such as netmums.com.
    - Collaborative spaces, such as Facebook.
    - Media sharing services, such as YouTube.
    - 'Micro-blogging' applications, such as Twitter.

- 3.2 Tibberton & St Lawrence School defines “cyber bullying” as any use of social media or communication technology to bully an individual or group.
- 3.3 Tibberton & St Lawrence CE Primary School defines “members of the school community” as any teacher, member of support staff, pupil, parent/carer of pupil, governor or ex-pupil.

4 Training of Staff

- 4.1 At Tibberton & St Lawrence recognise that early intervention can protect pupils who may be at risk of cyber bullying or negative social media behaviour. As such, teachers will receive training in identifying potentially at-risk pupils.
- 4.2 Teachers and support staff will receive training on the Social Media Policy as part of their new starter induction.
- 4.3 Teachers and support staff will receive regular and ongoing training as part of their development.

5 Pupil Expectations

- 5.1 Pupils are responsible for following the school rules and will be expected to follow requests from teachers.

6 Social Media Use – Staff

- 6.1 Staff may not access social media during lesson time, unless it is part of a curriculum activity.
- 6.2 Staff may use social media during their break times on their personal devices.
- 6.3 Members of staff should avoid using social media in front of pupils.
- 6.4 Members of staff **must not** “friend” or otherwise contact pupils or parents/carers through social media.
- 6.5 If pupils or parents/carers attempt to “friend” or otherwise contact members of staff through social media, they should be reported to the headteacher.
- 6.6 Members of staff should avoid identifying themselves as an employee of Tibberton & St Lawrence on social media.
- 6.7 Members of staff **must not** post content online which is damaging to the school or any of its staff or pupils.
- 6.8 Where teachers or members of staff use social media in a personal capacity, they should make it clear that their views are personal.
- 6.9 Teachers or members of staff must not post any information which could identify a pupil, class or the school.
- 6.10 Members of staff should not post anonymously or under an alias to evade the guidance given in this policy.
- 6.11 Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal.
- 6.12 Members of staff should be aware that if their out-of-work activity brings Tibberton & St Lawrence into disrepute, disciplinary action will be taken.
- 6.13 Members of staff should regularly check their online presence for negative content via search engines.
- 6.14 If inappropriate content is accessed online, an inappropriate website content report form should be completed and passed on to the Head of School.

- 6.15 Attempts to bully, coerce or manipulate members of the school community, via social media, by teachers and members of staff will be dealt with as a disciplinary matter.
- 6.16 Members of staff should not leave a computer or other device logged in when away from their desk, or save passwords.

7 Social Media Use – Pupils and Parents/Carers

- 7.1 Pupils may not access social media during lesson time, unless it is part of a curriculum activity.
- 7.2 Breaches of this policy by pupils will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to exclusion.
- 7.3 Pupils and parents/carers **must not** attempt to "friend" or otherwise contact members of staff through social media. If attempts to contact members of staff through social media are made, they will be reported to the headteacher.
- 7.4 If members of staff attempt to "friend" or otherwise contact pupils or parents/carers through social media, they should be reported to the headteacher.
- 7.5 Pupils and parents/carers should not post anonymously or under an alias to evade the guidance given in this policy.
- 7.6 Pupils and parents/carers **must not** post content online which is damaging to the school or any of its staff or pupils.
- 7.7 Pupils must not sign up to social media sites that have an age restriction above the pupil's age.
- 7.8 If inappropriate content is accessed online on school premises, it **must** be reported to a teacher.

8 Blocked Content on School Systems

- 8.1 All social networking sites are blocked for use by the pupils. This is a blanket ban for all forums and social networking. The only exception is 'wikispaces' which can be accessed. Youtube and pin-interest are open to staff only.
- 8.2 Attempts to circumvent the network's firewalls will result in a ban from using school computing equipment, other than with close supervision.
- 8.3 Inappropriate content which is accessed on the school computers should be reported to the headteacher so that the site can be blocked.
- 8.4 Requests may be made to access erroneously blocked content by request to Mrs North or Mrs Moore
- 8.5 The final decision on whether access should be granted to a site will be made by the headteacher.

9 Cyber bullying

- 9.1 At Tibberton & St Lawrence, cyber bullying is taken seriously.
- 9.2 Incidents of cyber bullying will be dealt with and reported along the same chain as the Anti-Bullying Policy.
- 9.3 Staff members should never respond or retaliate to cyberbullying incidents. Incidents should instead be reported as inappropriate, and support sought from their line manager or senior staff member.
- 9.4 Evidence from the incident should be saved, including screen prints of messages or web pages, and the time and date of the incident.

- 9.5 Where the perpetrator is a current pupil or colleague, most cases can be dealt with through the school's own disciplinary procedures.
- 9.6 Where the perpetrator is an adult, in nearly all cases, a senior staff member should invite the victim to a meeting to address their concerns. Where appropriate, the perpetrator will be asked to remove the offensive content.
- 9.7 If the perpetrator refuses to comply, it is up to the school to decide what to do next. This could include contacting the internet service provider in question through their reporting mechanisms, if the offensive content breaches their terms and conditions.
- 9.8 If the material is threatening, abusive, sexist, of a sexual nature or constitutes a hate crime, the school should consider contacting the police.
- 9.9 As part of our on-going commitment to the prevention of cyber bullying, regular education and discussion about e-safety will take place as part of computing and PSHCE.

10 Be SMART Online

We encourage pupils to take a SMART approach to social media behaviour:

- **Safe** – Do not give out personal information, or post photos of yourself to people you talk to online. Follow age restriction rules.
- **Meeting** – Do not meet somebody you have only met online. We encourage parents/carers to speak regularly to their children about who they are talking to online.
- **Accepting** – We advise that pupils only open emails and other forms of communication from people they already know.
- **Reliable** – We teach pupils about the dangers of believing everything they see online.
- **Tell** – We encourage pupils to tell a teacher, parent or carer if they see anything online that makes them feel uncomfortable.

Use of Internet

The use of the internet is a valuable business tool, but staff must be aware that the internet should be used responsibly.

Key Messages

- All internet use via the Council's equipment/systems will be monitored.
- Officers can only use the Council's internet facility for personal use in non-work time and in compliance with the usage set out in this document.
- Misuse of the internet can lead to disciplinary or criminal proceedings

Internet Acceptable Use

Staff **must**:

- ✓ Only access the internet for personal reasons in non-work time with access complying with the requirements of this policy.
- ✓ Ensure personal use of the internet complies with the requirements of this document.
- ✓ Consult with ICT before downloading software from the internet.
- ✓ Report any information found on the internet that may be inaccurate or defamatory to the Council or its officers to their line manager
- ✓ Report accidental unauthorised internet access, i.e. when they receive an 'Access Denied' system message, to their line manager

Internet Unacceptable Use

Staff **must NOT** use the Internet to:

- ✗ Breach the confidentiality of individuals or the Council
- ✗ Run a business or profit making activity including auction sites
- ✗ Access websites for personal use during work hours
- ✗ View websites that are not allowed by the Council on Council equipment/using Council infrastructure, including but not limited to:
  - Video and audio files
  - Photo searches
  - Sexually explicit/pornographic
  - Intolerance/Hate
  - Criminal action
  - Tasteless/Offensive
  - Chat groups/rooms
  - Violence/Weapons
  - Illegal Drugs
  - Hacking
  - Spyware
  - Proxies and translators
  - Sex education
  - Fraud
  - Phishing (fraudulently obtaining sensitive information such as passwords, bank details, etc, by pretending to be a trustworthy source)
- ✗ Download software or utilities to corporate equipment without authorisation
- ✗ Publish or make available confidential or personal data via websites, newsgroups, forums, social networking/media sites or any similar facility. For guidance on the appropriate use of social media sites please see the Social Media Policy.
- ✗ Represent their own opinions as those of the Council on any websites

✗ Knowingly distribute or otherwise be involved in virus, Trojans or other malware use.

Internet Monitoring

The Council reserves the right to monitor the use of the Internet and web in line with the Lawful Business Practice Regulations (2000) for the purposes of:

- gaining routine access to business communications
- monitoring standards of service and training
- prevention or detection of crime
- detecting unauthorised use of the internet.

Staff must be aware that the Council cannot guarantee privacy of staff private information if they use webmail or Internet banking and supply passwords and other security details to gain access to these facilities.

The Council reserves the right to block access to any website deemed inappropriate and to report access of inappropriate material to Human Resources/Audit & Governance in the event that this type of activity is logged. Misuse of the internet can lead to disciplinary action being taken.

Use of Email/Skype/Other Communication Technologies

Email/Skype for Business and other communication technologies are a valuable business tool. However staff must be aware that emails, saved Skype conversations and other electronic messages have the same legal status as other documents and in particular email attachments may be shared very quickly to readers across the world. Remember that contents of emails and/or any saved conversations using Skype or other communication technologies can be disclosed when requested under the Freedom of Information Act 2000.

Good management of staff mailboxes is essential for proper records management. It is also important as size of files and storage can easily get out of control, costing the Council time and money. The Council reserves the right to impose mailbox quotas on any or all staff in the event that storage becomes an issue.

IMPORTANT - Private Usage

Limited personal use of the Council's email system, Skype and other communication technologies is acceptable but this use must be confined to outside an officers working hours and staff must still abide by Council rules on acceptable and unacceptable use set out below.

Acceptable Use

Staff **must**:

- ✓ Use the Council's Secure Communication System (SCS) to exchange personal and sensitive data to external parties where GCSX cannot be used
- ✓ Ensure that a generic/team email account is only used in appropriate circumstances such as information which is relevant to each team member and not using the account to send confidential information which should only be shared with certain team members
- ✓ Ensure they send an email to the correct person, always double check the recipient. They must also limit the number of recipients of the email to people who require it to do their job or are bona fide recipients
- ✓ Limit the amount of personal data in the body of the email or in attachments to only that which is needed
- ✓ Where possible provide a link to documents in an email to reduce the number of copies held of a document
- ✓ Remind the recipient, if any sensitive/confidential data, of their responsibility for the security and confidentiality of that data
- ✓ When confidential/sensitive data is received by email it should be deleted from the email system as soon as possible and filed/secured appropriately, either electronically or on paper
- ✓ When "forwarding" emails or using the "reply all" facility consider whether the content is suitable for everyone on the list of recipients, as confidential/sensitive data could be sent in error
- ✓ Only use "bcc" (blind copy) in an email on an exception basis, after careful consideration - the message may be forwarded by the recipient as "reply all" to the "bcc". This would mean that all details will be revealed to the other people on that email list
- ✓ Use a dedicated room when using Skype video
- ✓ Only use Skype video for work purposes

Unacceptable Use

Staff **must not**:

- ✗ Use their Council email address for personal use, e.g. register it on a non-work website
- ✗ Respond to suspicious (spam) emails, if they have any doubts about who has sent the email then the email should not be opened or replied to
- ✗ Click on any untrusted web links detailed in a suspicious email or open any attachment as they may contain viruses.
- ✗ Use email/Skype/other communication tools to send personal messages in work time and/or that are inappropriate, abusive and malicious

- ✗ Access an email/Skype/other communication tool for which they are not authorised
- ✗ Use email/Skype/other communication tools for any private gain including running a business or associated advertising
- ✗ Keep received, sent or deleted sensitive/confidential data on the email/Skype/other communication tools longer than necessary
- ✗ Send or forward chain emails or those containing discriminatory or offensive material
- ✗ Send or forward confidential information outside the Council without appropriate security in place including strong passwords and encryption, e.g. use of SCS or GCSX
- ✗ Forward Council emails to their own personal email address
- ✗ Use the Councils email/ Skype/other communication tools in any way that could damage the reputation of the Council and/or its staff
- ✗ Represent their own opinions as those of the authority
- ✗ Send emails which infer that they are an official document when that is clearly not the case.
- ✗ Click on any links or follow any instruction in an email received from an unknown source. Emails of this nature can contain malicious content, if officers are unsure as to whether they should open an email or follow any subsequent instruction they should contact ICT

Security & Monitoring

Key Messages

- All emails sent and received using the Council's system will be automatically scanned and filtered.
- Officers emails/Skype messages and other electronic communications will be monitored if it is deemed appropriate to do so. This will include any private emails
- Misuse of email/Skype/other communication technologies can lead to disciplinary or criminal proceedings
- All emails/Skype and other messages communicated electronically on Council systems remain the property of the Council and may need to be disclosed under the Freedom of Information Act 2000

Security:

- Private, confidential, personal or sensitive information should not be revealed or sent by email except to Telford & Wrekin staff and/or school staff also on the same email system, i.e. all staff with an @telford.gov.uk or @taw.org.uk. When unsure whether content is suitable for sending by external email ask yourself "*if this information was about me, my family or my company would I want the information available for anyone to see?*"

- Secure email systems such as government connect (GCSX) and the Council's Secure Communication System (SCS) exist for the secure transfer of personal / sensitive information to external bodies and therefore should be used.
- Before sending emails staff must consider whether it is essential to include full names in external emails where abbreviations or reference numbers could be used, so that individuals cannot be identified.
- An email should be treated in the same way as a paper record regarding retention or deletion. Further information on retention/deletion of records can be provided by Information Governance.

Scanning/Monitoring:

- If any emails are stopped by the content filter they may be read by an appropriate ICT officer, if the decision to stop the email is challenged.
- The Council reserves the right to access, read and monitor emails/Skype messages or other electronic communications that are transmitted over Council networks or stored on Council equipment.
- Monitoring of activity will take place, in line with Lawful Business Practice Regulations 2000 and only when it is appropriate to do so.
- Misuse of email/Skype/other electronic communication technologies could result in temporary or permanent withdrawal of access and may be dealt with under the disciplinary process of the Council. Separate legal proceedings may be necessary including seeking prosecution under the Computer Misuse Act 1990.
- Email/saved Skype or other electronic messages may need to be accessed by management when staff are absent from work, and signing this policy will constitute acceptance of this.

'Out of Office' assistant should always be used for planned absence. All out of office messages should comply with Corporate Communications requirements and must contain as a minimum the statement *"If this is a request under the Freedom of Information Act or similar legislation, please send your request to foi@telford.gov.uk*". Where absence is unplanned officers should activate their out of office message via a works mobile device or by Web Mail. If this is unachievable managers will ask ICT to activate the 'Out of Office' message.

Outlook Calendars

With the move to Office 365 officers should not save personally identifiable data in the subject of their outlook calendars. Any exceptions to this must be approved by the relevant Assistant Director (Information Asset Owner).