

ST GEORGE'S
JUNIOR SCHOOL
SHREWSBURY

St George's Junior School

Social Media/Acceptable Use Policy 2021

Writing and reviewing the Social Media/Acceptable Use Policy

This policy relates to other policies including, E-Safety policy, Teaching and Learning Policy and Disciplinary Policy and procedures.

It has been agreed by senior leadership and approved by governors. This policy and its implementation will be reviewed annually.

All staff and workers at the school need to be aware of the risks and accountability of inappropriate or inadvertent provision of information about themselves, the school or its pupils and staff or the wider school community in the Social Media arena.

Every employee or volunteer working within the school setting is accountable for information published and must be aware that the Headteacher or a named representative may monitor such information.

It is important to note that information available in the public domain which has the potential for harm, distress or reputational damage may lead to disciplinary action being taken.

What is Social Networking and Social Media?

Social networking and social media are communication tools based on websites or networks which allow you to share information or other material about yourself and your interests with groups of other people.

These groups of people could be, but not limited to:

People who are known to you (friends or colleagues)
People you don't know but who share common interests (such as teaching, working in Telford)
Anyone who could find your comments through search engines.

Examples of Social Media and Social Networking sites and services include, but not limited to:

- Facebook
- Twitter
- YouTube
- LinkedIn
- Blogs
- Discussion groups
- Mailing Lists
- WhatsApp Messenger
- Instagram

What social media activity does this policy cover?

This policy is mainly concerned about two types of Social Media activity:

Your own personal activity, done for your friends and contacts, but not under or in the name of St. George's Junior School (or Empower Trust).

Activity carried out in the name of St George's Junior School, such as a school blog, website, Seesaw, Twitter posting or a Facebook group that represents, or appears to represent, the official views of the school.

This policy is not about stopping the use of – or accessing of – such groups, but aims to ensure that the use of social media does not harm the interests of the children and young people we support, or damages the reputation of the school or school staff.

Aim of this policy

This policy recognises that social media is an integral and growing part of everyday life and makes important contribution to teaching and learning opportunities. However, the rapid evolution of social networking technologies requires a robust policy framework and this policy aims to:

- Assist staff working with children to work safely and responsibly with the internet and other communication
  technologies to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary and/or legal action will be taken
- Support safe working practice
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils
- Prevent adults abusing or misusing their position of trust

This document applies to all staff who work in the school whether paid or unpaid and includes members of the Governing Body.

Principles

The principles that underpin this policy are:

- Adults who work with pupils are responsible for their own actions and behaviour and must avoid any conduct which would lead any reasonable person to question their motivation and intentions.
- Adults in the school must work and be seen to work, in an open and transparent way.
- Adults in the school must continually monitor and review their own practice in terms of the continually
  evolving world of social networking and ensure that they consistently follow the guidance contained in the document.

Why do we need the policy?

There have been numerous examples of people in all walks of life posting things in social media that they have later regretted because that information has harmed or put at risk themselves or others. This includes:

- Accidentally posting personal or embarrassing information about themselves or others in a public forum or beyond the group the information was originally intended for
- Sharing information about yourself or others with people you don't know that could be used by someone to commit fraud or misrepresent the views of yourself or others (such as identity theft)
- Breaching privacy or child protection laws and regulations or workplace policies by posting information about your work or the children and adults that you work with
- You or others receiving negative publicity, harassment, inappropriate contact or threats as a result of your views, beliefs or comments.

This has led to people facing disciplinary actions, losing their jobs, being prosecuted or even imprisoned.
This policy and guidance will help to make sure that your use of social networking sites and social media is safe.

Safer Social Networking Practice

This document applies to current social networking sites such as Facebook, Twitter, Instagram etc and all other current and emerging social media platforms.

All staff and volunteers must adhere to, and apply the principles of this document in all aspects of their work. Failure to do so may lead to action being taken under the disciplinary procedure.

Social Networking "Must Nots"

- Staff or volunteers must not make comments on behalf of the school or claim to represent the views of the school, unless they have explicit permission to do so
- Staff or volunteers should never make a 'friend' of a pupil at the school where they are working on their social networking page and seek the advice of the Headteacher before becoming 'friends' with ex-students once they reach adulthood.
- Staff or volunteers should not be a 'friend' of a parent/carer of a pupil or ex-pupil of the school without seeking advice of the Headteacher.
- Staff or volunteers should never use or access social networking pages of pupils
- Staff or volunteers must not request, or respond to, any personal information from a pupil
- Staff or volunteers should never post confidential information about themselves, the school, the governing body, the Local Authority, the academy trust, their colleagues, or their pupils. If they are posting in an 'official' capacity, they should not post confidential information about members of the public.
- Staff and volunteers should not make allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or another school, or the Trust. Doing so may results in disciplinary action being taken against them. If they have concerns about practices within the school or the actions of pupils or parents, they must act in accordance with the local Trust's Whistle-Blowing Policy and the school's complaints procedure.
- Staff members or volunteers must not send inappropriate images, sexually inappropriate comments or comments that can be misconstrued to other staff members via any social media or online communication platform.
- Staff should refrain from swearing and having inappropriate images on their social media accounts that are set to public.

Social Networking "Shoulds"

- All adults, particularly those new to the school setting, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes photographs that may cause embarrassment to themselves and/or the school if they were to be published outside of the site.
- In their own interests, adults within school settings need to be aware of the dangers of putting their personal information onto social networking sites such as addresses, home or mobile phone numbers. This will avoid the potential for pupils or their associated families/friends having access to staff outside the school environment. It also reduces the potential for identity theft by third parties.
- There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle. These contacts, however, will be easily recognised and should be openly acknowledged with the Headteacher where there may be implications for the adult and their position within the school setting.
- On leaving employment from the school, staff should review their social networking sites to ensure information relating to the school is accurate and appropriate.

Social Networking Good Practice

Staff and volunteers must understand who is allowed to view the content on their pages of any sites they use and how to restrict access to certain groups of people.

- On Facebook, they should understand whether the posts they make are Public (anyone can see them), visible to Friends (only people on their Friends list can see them) or visible to Friends of

Friends, which means that posts are visible to all the friends of friends, which could be many hundreds or even thousands of people.

- On Twitter and LinkedIn, all posts, unless they are direct messages to another user, are visible to everyone (the whole world)
- If you are unsure of who can see your posts on other sites, you should always assume that the information is publically available to all and could be found by people doing a search on Google, for example:

Before posting, staff and volunteers should ask themselves the following questions:

1. Do you want the whole world to see? Even if you restrict your own visibility settings, these can be overridden by the settings of others, or people can copy and paste the information into other, public places.
2. Do you want the post to be seen forever? Once you have posted something, it is almost impossible to delete it again from the internet, even if you delete it from the site. There are sites that archive all Twitter posts, for example, so even if you delete a post from Twitter, it can still be found.
3. What if the information is taken out of context? It is very easy for others to take what is posted, alter it, and re-post it elsewhere. It is also possible that your hard work, posted online, may be used inappropriately by others.
4. Could the information put you or others in danger? What you post could tell others that your house is empty or that the pupils in your class are on a school trip, which could have implications for a looked-after child.
5. Are you violating any laws? The information could breach copyright, or specific legislation relating to privacy of vulnerable groups, for example.
6. Is your message clear? Could you unintentionally be breaking cultural norms or putting out something unintentionally offensive. Is it clear whether or not you are posting in an official capacity?
7. Could the actions of your social networking friends reflect on you? Could your friends or friends of friends "tag" you in photographs or link you to inappropriate activities through their own posts?

If you have any doubts about any of these points, you should seek the advice of the Headteacher, Deputy or E-safety Lead.

Cyberbullying

It is important for all staff to understand the issues related to cyber bullying given that they as well as pupils may become targets. Cyberbullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'

If cyberbullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. Employees are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.

Employees are encouraged to report any and all incidents of cyberbullying to their line manager or the Headteacher. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police. Employees may wish to seek the support of their trade union or professional association representatives.

If the staff member or volunteer becomes aware of a pupil being subject to cyberbullying, they should raise it with their line manager or Headteacher. If the alleged perpetrator is the Headteacher, then incidents should be reported to the Chair of Governors.

Staff, Governors and Visitors Agreement

I agree that **I will**:

- Only use, move and share personal data securely.
- Respect the school network security.
- Implement the school's policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources.
- Respect the copyright and intellectual property rights of others.
- Only use approved email accounts for school.
- Only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site.
- Only give permission to pupils to communicate online with trusted users.
- Use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- Not share my personal (home) accounts/data (eg face-book, email, e-bay, etc.) with pupils.
- Set strong passwords which I will not share and will change regularly (a strong password is a minimum of 6 characters, one which uses a combination of letters, numbers and other permitted signs).
- Report unsuitable content and/or ICT misuse to the named e-safety officer.
- Promote any supplied e-safety guidance appropriately.

I know that anything I share online may be monitored.
I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I agree that I **will not**:

- Visit internet sites, make, promote, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - Pornography (including child pornography).
    - Promoting discrimination of any kind.
    - Promoting violence or bullying.
    - Promoting racial or religious hatred.
    - Promoting illegal acts.

- Breach any Local Authority/School policies, eg Gambling.
- Make derogatory comments or 'like' derogatory comments about the school with reference to governors, staff or pupils via social media sites (eg Facebook, twitter, etc).
- Do anything which exposes others to online dangers.
- Post any other information which may be offensive to others.
- Forward chain letters.
- Breach copyright law.
- Use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission from the Headteacher.
- Store images or other files off site without permission from the Headteacher or his/her delegated representative.

I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.

I understand that the data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used in any investigation.

Signed: _____ Date: _____

Name: _____