Evergreen School

STAFF ACCEPTABLE USE & SOCIAL MEDIA POLICY

Approved By: Governing Body Approved on: 25/11/20 Review Due: October 2023

1. INTRODUCTION

1.1 The internet e-mail and social media play an essential role in the conduct of our business in school. The systems within school are made available to students, teaching staff, support staff and other authorised persons to further enhance both educational and professional activities including teaching, research, administration and management. We value the ability to communicate with colleagues, pupils and business contacts.

1.2 How we communicate with people not only reflects on us as individuals but on the School. Therefore, although we respect your personal autonomy and privacy, we have established this policy to ensure that you know what we expect from you and what you can expect from us in your use of e-mail, social media and the internet.

1.3 We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this Policy.

1.4 For your safety, we are able to monitor all web pages visited, email sent and received. This helps us monitor inappropriate use, such as bullying.

1.5 This policy applies to you as an employee whatever your position, whether you are a Head Teacher, Teacher, support staff, permanent, temporary or otherwise. Any inappropriate use of the School's internet & e-mail systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal.

1.6 It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Head Teacher or your line manager.

2. GENERAL PRINCIPLES AND LEGAL ISSUES

2.1 All information relating to our pupils, parents and staff is confidential. You must treat all School information with the utmost care whether held on paper or electronically.

2.2 Care must be taken when using e-mail as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school. Electronic information can be produced in court in the same way as oral or written statements.

2.3 We trust you to use the internet sensibly. Please be aware at all times that when visiting an internet site, the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school.

2.4 The main advantage of the internet and e-mail is that they provide routes to access and disseminate information. However, the same principles apply to information exchanged electronically in this way as apply to any other means of communication. For example, sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.

2.5 Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your headteacher.

2.6 As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the School where it is necessary for your duties. The processing of personal data is governed by the Data Protection Act 2018. Schools are defined in law as separate legal entities for the purposes of complying with the Data Protection Act. Therefore, it is the responsibility of the School, and not the Local Authority, to ensure that compliance is achieved.

2.7 All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

3. MONITORING COMMUNICATIONS

3.1 This policy takes into account legislation which aims to ensure a minimum level of personal privacy for employees in their employment. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 allows for interception of "business" communications for business purposes:

3.1.1 to establish the existence of facts
3.1.2 to ascertain compliance with applicable regulatory or self-regulatory practices or procedures.
3.1.3 to ascertain or demonstrate effective system operation technically and by users.
3.1.4 for national security/crime prevention or detection.
3.1.5 for confidential counselling/support services.
3.1.6 for Investigating or detecting unauthorized use of the system
3.1.7 for monitoring communications for the purpose of determining whether they are communications relevant to the business.
3.2 Warwickshire LA has an obligation to monitor the use of the internet and e-mail services provided as part of the Warwickshire Broadband service to schools, in accordance with the above Regulations. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. Warwickshire LA and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from employees the facility to send and receive electronic communications

3.3 If employees wish to identify certain emails as personal, it is their responsibility to clearly mark the email as personal. However, WCC reserves the right to examine such emails as part of a wider investigation and will not be viewed unless legitimate reason to do so.It is good practice to use the word `personal' in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.

3.4 Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the School's business purposes which include the following:
3.4.1 providing evidence of business transactions;
3.4.2 making sure the School's business procedures are adhered to;
3.4.3 training and monitoring standards of service;
3.4.4 preventing or detecting unauthorised use of the communications systems or criminal activities.
3.4.5 maintaining the effective operation of communication systems.

4. USE OF INTERNET AND INTRANET

4.1 When entering an internet site, always read and comply with the terms and conditions governing its use.

4.2 Do not download any images, text or material which is copyright protected without the appropriate authorisation.

4.3 Do not download any images, text or material which is inappropriate or likely to cause offence.

4.4 If you want to download any software, first seek permission from the Head Teacher and/or member of staff responsible. They should check that the source is safe and appropriately licensed.

4.5 If you are involved in creating, amending or deleting our web pages or content on our web sites, such actions should be consistent with your responsibilities and be in the best interests of the School.

4.6 You are expressly prohibited from:

4.6.1 introducing packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
4.6.2 seeking to gain access to restricted areas of the network;
4.6.3 knowingly seeking to access data which you are not authorised to view;
4.6.4 introducing any form of computer viruses;
4.6.5 carrying out other hacking activities.
4.7 For your information, the following activities are criminal offences under the Computer Misuse Act 1990:
4.7.1 unauthorized access to computer material i.e. hacking;
4.7.2 unauthorized modification of computer material;
4.7.3 unauthorized access with intent to commit/facilitate the commission of further offences.

5.USE OF E-MAIL

5.1 You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.

5.2 Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is `Confidential@ in the subject line.

5.3 Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.

5.4 Do not impersonate any other person when using e-mail or amend any messages received.

5.5 It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.

6. DATA PROTECTION

6.1 Through your work personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the School's premises or working remotely you must:
6.1.1 Keep the data private and confidential and you must not disclose information to any other person unless authorized to do so. If in doubt, ask your Head Teacher or line manager;
6.1.2 familiarize yourself with the provisions of the Data Protection Act 2018 and comply with its provisions;
6.1.3 familiarize yourself with all appropriate School policies and procedures;
6.1.4 not make personal or other inappropriate remarks about staff, pupils, parents or colleagues on manual files or computer records. The individuals have the right to see all information the School holds on them subject to any exemptions that may apply.
6.2 The School views any breach of the Data Protection Act 2018 as gross misconduct which may lead to summary dismissal under appropriate disciplinary procedures.
6.3 If you make or encourage another person to make an unauthorized disclosure knowingly or recklessly you may be held criminally liable.

7 **Social Media**

7.1 Social media includes online social forums such as Facebook, Twitter and LinkedIn and websites such as YouTube and Flickr. This type of media which is now widely used allows people to communicate instantly and share data in a public forum.

7.2 There are many more examples of social media than can be listed here and this is a constantly changing area. Staff should comply with this Policy in relation to any social media that they use.

7.3 The term “staff” in this document, should also be read to include any contractors or volunteers at the school. There is a separate section in relation to school governors towards the end of this document.

7.4 In using social networking and internet sites, clear and explicit professional boundaries will be adhered to as outlined in Section 12 of ‘Guidance for Safer Working Practice for those working with Children and Young People in Education Settings’ (Safer Recruitment Consortium 2015), which can

be found at the following link
http://www.saferrecruitmentconsortium.org/GSWP%20Oct%202015.pdf

7.5 Personal use of social media at work

Staff are not allowed to access social media websites from the School's computers or devices at any time. [This includes [laptop/palm-top/hand-held] computers or devices distributed by the School for work purposes.]

The School understands that staff may wish to use their own computers or devices, such as laptops and palm-top and hand-held devices, to access social media websites while they are at work. Staff must limit their use of social media on their own equipment to their official rest breaks (such as their lunch break) and must still ensure that they continue to follow the requirements set out in this Policy.

If it is believed a member of staff has engaged in unlawful activity on a social media site or activity in breach of this Policy and the Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings, Section 12, communication with pupils (see link in 1.5) an investigation will be instigated which may result in disciplinary action and potentially dismissal. The School's disciplinary policy will be followed.

7.6 Use of social media and the internet for work purposes

In specific circumstances it may be appropriate for a member of staff to use social media as part of their work. This should only take place with the approval of the Head, Deputy or Assistant Head teacher. In such circumstances while contributing to the School's social media activities the same safeguards must be adhered to as would be with any other form of communication about the School in the public domain. Any communications made in a professional capacity through social media must not either knowingly or recklessly:

Place a child or young person at risk of harm;
Bring the School into disrepute;
Breach confidentiality;
Breach copyright;
Breach data protection legislation; or
Do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:

- making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
- using social media to bully another individual; or
- posting images that are discriminatory or offensive or links to such content.

7.7 Excessive use of social media/internet at work

Staff must not spend an excessive amount of time while at the School on personal use of social media or internet sites. They must ensure that use of social media/internet does not interfere with their duties.

7.8 Monitoring use of social media/internet on school equipment during work time

The School reserves the right to monitor staff internet usage. The School considers that valid reasons for checking internet usage include concerns that social media/internet sites have been accessed in breach of this Policy.

7.9 Inappropriate use of social media/internet

The following list gives examples of use of social media/internet sites that the school may consider to be inappropriate:

Publishing defamatory; discriminatory; illegal; sexual; racist or other offensive material;
Publishing any material which is confidential or would breach copyright or data protection principles;
Promoting personal financial interests, commercial ventures or personal campaigns in school time;
Publishing anything of an abusive or harassing nature;
Using social media/internet sites in a manner that would put staff/governors in breach of school codes of conduct or existing policies;

Discussing matters relating to school, staff, pupils or parents/carers for which the social media is not considered to be an appropriate forum;
Inappropriately holding yourself out as, or implying that you are, a representative of the school when using social media/internet sites in a private context;
Interacting with pupils via social media/internet sites [*unless properly authorised as part of school duties];*
Interacting with parents/carers of pupils via social media/internet sites;
Interacting with any ex-student who is under the age of 18 (staff should exercise extreme caution in interacting with any ex-pupils regardless of age);
Actively providing false or misleading information about the school, its staff or pupils;
Cyber-bullying;
Inappropriately referencing other staff members, governors, students, parents or school activities/events - unless it is a legitimate part of the staff member's role;
Using social media/internet sites to raise complaints/grievances – any issues should be raised via the appropriate channels (e.g. school complaints procedure).

The above is a non-exhaustive list. It is intended to provide some examples of what the School considers to be inappropriate. Each matter will be dealt with based on its own facts. School policies will be followed where relevant (e.g. the School's disciplinary/bullying /complaints policy etc). The School will contact the Police where it is necessary to do so.

7.10 Social media in your personal life

The School recognises that many people make use of social media in a personal capacity. While they are not acting on behalf of the School, staff must be aware of the potential damage that could be caused to the School if they are recognised as being a member of staff.

Staff may say that they work for the School but their online profile (for example, the name of a blog or a Twitter name) must not contain the School's name.

If staff do discuss their work on social media (for example, giving opinions on their specialism or the sector in which the School operates), where appropriate they should include on their profile a statement along the following lines: "The views I express here are mine alone and do not necessarily reflect the views of the School."

Any communications that staff make in a personal capacity through social media must not bring the School into disrepute.

7.11 Disciplinary action over social media use

All staff are required to adhere to this policy. Staff should note that any breaches of this policy may lead to disciplinary action. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing serious damage to the School, may constitute gross misconduct and lead to summary dismissal.

Similarly, where there is a serious breach of this policy, action may be taken in respect of other members of staff who are not employees which may result in the termination of their appointment.

Staff have a duty to report abuses of this policy in accordance with the schools whistleblowing policy.

7.12 Child protection guidance

If the head teacher (*or other member of staff*) receives a disclosure that a member of the School's staff is using a social networking/internet site in a way that may put a child at risk, this should be recorded in line with the School's child protection policy and whistleblowing policy as an allegation. In accordance with *the Department for Education's (DfE)* Working Together to Safeguard Young

People (2015), the head teacher will refer all allegations of a safeguarding nature to the Designated Officer (DO) in the Local Authority before undertaking any internal investigations.

[*Designated Officer – via MASH on 01926 742006 or* mash@warwickshire.gov.uk].

7.13 Staff/governors interacting with each other online

Governors are advised not to be "friends" with members of staff online. Reasons for this include:

Potential for a conflict of interest where a governor is on a selection panel/disciplinary panel where a "friend" is involved;

Due to the role of the governing body and its general responsibility for the conduct of the school, it is sensible to maintain a certain level of separation between governors and staff.

Teachers and other staff members should also exercise caution when considering inviting work colleagues to be 'friends' on social networking sites, as this may create a conflict/difficult situation in the future.

7.14 Application of this Policy to school governors

Whilst some aspects of this Policy are clearly more targeted at school staff, many have equal application to governors. For example, section 7 of the Policy provides guidance for all on what is considered to be inappropriate use of social media/internet sites. All governors should ensure that they comply with the spirit of the Policy.

Though governors would not be subject to the same disciplinary process as staff, there are still forms of redress available where a governor behaves in an inappropriate manner. The appropriate procedures would be followed in such cases.

7.15 Involvement with the PTA

This policy will continue to apply to members of staff who are acting in their capacity as a member of Parent-Teacher Association (PTA). Therefore they should ensure that they are acting in the spirit of this policy when acting in this capacity.