Heart of the Forest

Community Special School

Acceptable Use, Social Media and Mobile Phones

Approved by:	HoF Governing Body	Date:	Sept 25
Last reviewed on:	September 2022	Next review date:	Aug 25
Website:	Yes	Type:	Statutory

Staff (and Volunteer) Acceptable User

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

• that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

• that the school's systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

• that staff are protected from potential risk in their use of technology in their everyday work. The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students and will, in return, expect staff and volunteers to agree to be responsible users.

Adult Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

• I understand that the school will monitor my use of the school digital technology and communications systems.

• I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school

• I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

• I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

• I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

• I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

• I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

• I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information.

• I will only use social networking sites in school in accordance with the school's Social Media guidance in the Safeguarding Policy.

• I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.

• I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school.

• When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

• I will not use personal email addresses to correspond on school matters.

• I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

• I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the

Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless permission is gained from the Headteacher to do so.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others. Where digital personal data is transferred outside the secure local network, it must be password protected. Paper based Protected and Restricted data must be held in lockable storage.

- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when I am required by law or by the schools policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school.

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension,

referral to Governors or the Local Authority and in the event of illegal activities the involvement of the police. I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Social Media Use

Social Media is used increasingly across society and is recognised as a hugely valuable communication tool. However, the open nature of the internet means that social networking sites can leave professionals (such as teachers and other staff working in education) vulnerable if they fail to observe a few simple precautions. This policy is designed to protect school staff and pupils from potential harm or from becoming victims of radicalisation, extremism and malicious, upsetting or inadvisable contact.

Social media provide a range of social media tools that allow users to interact with one another.
It is recognised that there are benefits to effectively using social media for business and personal purposes.
This policy seeks to ensure that school staff use social media responsibly and to avoid them inadvertently placing themselves in a situation where their conduct is called into question due to unacceptable use of social media.

Social media is any type of interactive online media that allows parties to participate in interactive discussions and share information in a public forum. It is important to note that this may apply to some forums that are private but are shared or made public i.e. the policy may extend to 'closed groups' where a matter in breach of this policy is brought to the attention of the school.

Examples of some popular forums are Twitter, Facebook and LinkedIn, but social media also includes podcasts, open access online encyclopaedias, social bookmarking sites, blogs and video, live streaming forums and image-sharing websites such as YouTube, Vimeo, and Instagram. It is impossible to list all relevant media as this is a constantly changing and growing area.

This policy covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained by and on behalf of the school.

Social media relating to the school

Authorisation to share specific school business via communication channels which cannot be directly managed by the school (such as personal social media) must be sought from the head teacher/Governing Body of the School prior to sharing.
This includes opinions shared on social media that can be, or perceived to be, attributable to the school, its representatives and/or its decision-makers.

Sharing of any aspects of school business or relevant communications from the school via authorised social media platforms used and managed by the school must be approved by the head teacher.

Any authorised messages must be constructed to be unambiguous, accurate, politically neutral, fair and transparent if they are to formally represent the School or the County Council.

Creation of social media accounts by school staff for use in education
All social media services must be approved by the head teacher/Governing Body of the school in advance of any educational work being undertaken.

Personal use of social media by employees
It is accepted that employees and members of the school community will have their own social networking accounts. However, it is important that they protect their professional reputation, the reputation of the school and the privacy of colleagues, pupils and parents.
Staff **must not** identify themselves as employees of the school in their personal webspace apart from professional websites such as LinkedIn. This is to prevent information on these sites from being linked with the school and the County Council and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.

Employees are required to familiarise themselves with social network sites' privacy settings and are encouraged to make their settings 'private' and set the privacy levels as strictly as they can in order to ensure that information is not automatically shared with a wider audience than intended e.g. on Facebook opting out of public listings to protect their own privacy.
Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.
(Please see the "Social networking – Guidelines for NASUWT members which sets out minimum recommended privacy settings for Facebook)

Caution is advised when inviting work colleagues to be 'friends' on personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place.

Staff **must not** use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations, School or the County Council.

Employees must be aware that even with high privacy settings, their posts are never truly private as friends/connections could save or share these posts, so this policy may still apply even if the profile is private.

Conduct

Employees must not conduct or portray themselves, or allow friends to portray them, in a manner which may:

- bring the school into disrepute;
- lead to valid parental/carer complaints;
- be deemed as derogatory towards the school and/or its employees;
- be deemed as derogatory towards pupils, parents/carers or governors;
- bring into question their appropriateness to work with children (including behaviour that is illegal);
- contravene current National Teacher Standards (or other relevant professional standards).
- In addition to posts written by the employee, this can also include posts that the individual has shared, liked, retweeted etc. as well as tagged photographs where the content contravenes this policy.

Further to this staff should not:

- form online friendships or enter into communication with parents/carers as this could lead to professional relationships being compromised;
- form online friendships or enter into online communication with pupils as this could lead to professional relationships being compromised, and/or safeguarding allegations being raised;
- post pictures of or negative comments about their employment, school events (sharing information and posting pictures about school events should be done through the school's authorised social media site(s) or with advance authorisation from the head teacher/Governing Body).
- **make contact through any personal ICT or social medium with any pupil**, whether from our school or any other school, unless the pupil is your own family member OR an existing close family friend. School does not expect staff members to discontinue contact with their own family members or significant family friends via personal social media, however care should be taken not to communicate with friends of the family member who may be school pupils. Staff members **must decline 'friend requests' from pupils** they may receive in their personal social media accounts. Pupils/parents will be informed that this will be the case on induction.
- **have social media contact with any pupils' family members (parents/carers)** This is in-line with the NASUWT teachers' union and other unions which say that teachers should never under any circumstances accept Facebook friend requests from parents of a pupil.

It is recognised that employees may be known in the community in which they work and may have connections to parents/carers of pupils on social media (either relatives or close friends). Employees in this situation are responsible for their own social media and hold such connections at their own risk. Breaches under this policy in relation to this type of connection are managed in the same way.

Further Guidance
On leaving school employment, staff members **<u>must not</u>** contact pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal social media.

Any information staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues, County Council staff and other parties and service or County Council corporate information must not be discussed on their personal webspace or social media sites.

Photographs, videos or any other types of image of pupils and their families or images depicting staff members who can be identified as school staff must not be published on personal webspace or social media sites.

School or County Council email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

School logos or brands must not be used or published on personal webspace/social media sites (apart from professional websites such as LinkedIn)

School does not permit personal use of social media or the internet during core contracted work hours. Access to social media sites for personal reasons is not allowed between 9am and 4.15pm (apart from during lunch breaks). Staff members are expected to devote their contracted hours of work to their professional duties.

Parents/carers (the 'wider' school community) on social media sites
Parents/carers will be communicated with regarding their use of social media (in particular when they or a child they are responsible for joins the school) via the school website, letter and school newsletters particularly with regard to the following:
- Parents/carers are asked not to post images (photos and videos) of pupils other than their own children on social media sites unless they have the permission of parents/carers of other children pictured.
- Parents/carers are asked to raise queries, concerns or complaints directly with the school rather than posting them on social media.
- Parents/carers should not post malicious or fictitious comments on social media sites about any member of the school community.

While the school cannot monitor all use of social media in the wider school community the communication to parents/carer aims to protect pupils and staff at the school and the confidentiality of information about pupils and staff.
Dealing with incidents of online (cyber) bullying

Cases of online bullying will be dealt with in accordance with the school's policies and could lead to action being taken under the disciplinary procedure.

The school can take action with reference to any incident that takes place outside school hours if it:
- could have repercussions for the orderly running of the school,
- poses a threat to a member of the school community,
- could adversely affect the reputation of the school, or its employees/governors.

There are UK statutes that cover the use of Internet technology in relation to bullying.

Where cyber bulling involves pupils it may be necessary to deal with this under a separate policy (e.g. the schools' Anti-Bullying policy).

Where appropriate, legal action may be taken by the school's governors.

Mobile Phone Policy

At the Heart of the Forest we recognise that mobile phones, including smart phones, are an important part of everyday life for our pupils, parents and staff, as well as the wider school community.

This policy aims to:

- Promote, and set an example for, safe and responsible phone use

- Set clear guidelines for the use of mobile phones for pupils, staff, parents and volunteers

- Support the school's other policies, especially those related to child protection and behaviour

This policy also aims to address some of the challenges posed by mobile phones in school, such as:

- Risks to child protection

- Data protection issues

- Potential for lesson disruption

- Risk of theft, loss, or damage

- Appropriate use of technology in the classroom

Staff

All staff (including teachers, support staff, and supply staff) are responsible for enforcing this policy.

Volunteers, or anyone else otherwise engaged by the school, must alert a member of staff if they witness, or are aware of, a breach of this policy.

Use of mobile phones by staff

Personal mobile phones

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to make or receive calls, or send texts, while during contact time. Use of personal mobile phones must be restricted to non-contact time, and to areas of the school where pupils are not present (such as the staff room or PPA room).

Due to the lack of phone signal at the school where normally you would give your mobile for emergency contact, (e.g. child school or ill dependant) please give the school number 01594 822715

Data protection

Staff must not use their personal mobile phones to process personal data, or any other confidential school information.

Safeguarding

Staff must refrain from giving their personal contact details to parents or pupils, including connecting through social media and messaging apps.

Staff must avoid publicising their contact details on any social media platform or website, to avoid unwanted contact by parents or pupils.

Staff must not use their mobile phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil. If it's necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using school equipment.

Using personal mobiles for work purposes

In some circumstances, it may be appropriate for staff to use personal mobile phones for work. Such circumstances may include, but aren't limited to:

- Emergency evacuations
- Supervising off-site trips
- Supervising residential visits

In these circumstances, staff will:

- Use their mobile phones in an appropriate and professional manner, in line with our staff code of conduct
- Not use their phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil

- Refrain from using their phones to contact parents. If necessary, contact must be made via the school office

Work phones

Some members of staff are provided with a mobile phone by the school for work purposes.

Only authorised staff are permitted to use school phones, and access to the phone must not be provided to anyone without authorisation.

Staff must:

- Only use phone functions for work purposes, including making/receiving calls, sending/receiving emails or other communications, or using the internet

- Ensure that communication or conduct linked to the device is appropriate and professional at all times, in line with our staff code of conduct.

Use of mobile phones by parents, volunteers and visitors

Parents, visitors and volunteers (including governors and contractors) must adhere to this policy as it relates to staff if they are on the school site during the school day.

This means:

- Not taking pictures or recordings of pupils, unless it's a public event (such as a school fair), or of their own child

- Using any photographs or recordings for personal use only, and not posting on social media without consent

- Not using phones in lessons, or when working with pupils

Parents, visitors and volunteers will be informed of the rules for mobile phone use when they sign in at reception or attend a public event at school.

Parents or volunteers supervising school trips or residential visits must not:

- Use their phone to make contact with other parents

- Take photos or recordings of pupils, their work, or anything else which could identify a pupil

Parents or volunteers supervising trips are also responsible for enforcing the school's policy for pupils using their phones, as set out in section 4 above.

Parents must use the school office as the first point of contact if they need to get in touch with their child during the school day. They must not try to contact their child on his/her personal mobile during the school day.

Smart watches

Staff are permitted to wear smart watches but they must be unpaired from mobile phones during working hours.

Loss, theft or damage

The school accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while pupils are travelling to and from school.

Breaches of the policy

Any breach of this policy may lead to disciplinary action being taken against the staff member(s) involved in line with the School's disciplinary procedure.

Inappropriate use of social media by employees or volunteers should be referred to the head teacher/Board of Governors in the first instance so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the school and the County Council. In local authority community and voluntary controlled schools where there has been a breach of confidential information the breach must be reported to the Data Management team at Gloucestershire County Council.

A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of the School or the County Council or any illegal acts or acts that render the School or the County Council liable to third parties may result in disciplinary action and dismissal from service.

Any illegal acts may be reported to the police and/or the relevant professional body.

I have read and accept the terms of the:-
Acceptable Use, Social Media and Mobile Phone Policy for
all Permanent and Temporary Staff

Please tick to confirm you have read this policy

I understand the implications of any breach of this policy as outlined above.
Name (Printed): _____   Date: _____
Signature: _____