

North Nibley C of E Primary School

Acceptable Use of Technology and Social Media Policy

Policy status	Required by GCC Safeguarding Audit
Responsible for this policy	Teaching, Learning & Community
Policy reviewed/amended	January 2021
Policy review frequency	Every Three Years
Policy due for renew	January 2024

North Nibley Church of England Voluntary Aided Primary School, formerly the William Purnell Endowed School, was founded in the Eighteenth Century to provide education for the children of North Nibley and the surrounding villages.

Our Vision is to inspire and celebrate learning, achievement, faith and fun.

Ours is a school that works in partnership with the community to enable and equip each child to live life to the full, reflecting the Christian values of our foundation.

We will realise our Vision by:

- demonstrating, as a Church school, our Christian values in action
- providing a happy, healthy and secure environment where all are respected, valued and encouraged to contribute
- encouraging participation and a love of learning by offering experiences full of opportunity and creativity
- pursuing excellence in every aspect of school life, supporting one another and celebrating the achievements of all

This policy supports our vision by making clear that we are responsible for our actions, to keep ourselves and others free from harm and potential harm; that we have a responsibility to act wisely and respect the property that does not belong to us; to respect confidentiality and the rights of others.

A Biblical Perspective:

“Whatever you do, work heartily, as for the Lord and not for men.” **Colossians 3:23**

“For God gave us a spirit not of fear but of power and love and self-control.” **2 Timothy 1:7**

SAFEGUARDING STATEMENT

THIS POLICY IS PART OF OUR SUITE OF SAFEGUARDING POLICIES AND PROCEDURES.

IT MUST BE READ IN CONJUNCTION WITH THE FOLLOWING, MANY OF WHICH CAN BE FOUND ON OUR WEBSITE: www.northnibley.gloucs.sch.uk

- Acceptable Use of Technology & Social Media
- Allegations Management
- Anti-bullying, anti-hate and anti-radicalisation
- Attendance
- Behaviour
- Child Protection & Safeguarding Procedures (including COVID-19 measures)
- Children Missing Education
- Children who go missing during the school day
- Complaints
- Confidentiality
- Curriculum Policies - Computing and E-Safety
- Curriculum Policies - Drug Education
- Curriculum Policies – PSHE/Wellbeing
- Curriculum Policies - PE
- Curriculum Policies - Relationships and Sex Education
- Curriculum Policies - Science
- Curriculum Policies - Collective Worship
- Educational visits
- First Aid
- Health and Safety
- Intimate Care
- Keeping Children Safe in Education (Latest version)
- Medical Conditions and Support for those Unable to Attend School
- Offers of Early Help
- Physical Intervention
- Remote Teaching and Learning Policy
- Risk Assessments
- Safer Recruitment, Staff Selection and Induction
- Safer Working Practices
- Special Educational Needs and Disabilities
- Staff Code of Conduct & Staff Handbook
- Volunteer Policy and Codes of Conduct
- Whistleblowing
- Working Together to Keep Children Safe (Latest version)

“The School will fully engage in multi-agency working, in line with statutory guidance as outlined in the latest versions of “Keeping Children Safe in Education” (KCSIE), “Working Together to Safeguard Children” (Working Together) and local arrangements for child safeguarding in Gloucestershire. **Safeguarding is everyone’s responsibility.**”

Acceptable Use of Technology Policy

applicable for all adults working at school (Staff, Governors & Students)
and those using school hardware for the purposes of 'remote' learning.

As a professional organisation with responsibility for safeguarding, it is important that staff, governors and volunteers take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All adults have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that adults are fully aware of their professional responsibilities when using technology, they are asked to read this Acceptable Use Policy, and sign an acknowledgement slip.

This is not an exhaustive list; all adults are reminded that IT use should be consistent with the school ethos, school policies, national/local guidance and expectations, and the Law.

1. I understand that Information Systems and IT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites.
2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate. I will protect the devices in my care from unapproved access or theft.
4. I will respect system security and will not disclose any password or security information. I will use a 'strong' password to access school systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system. School will need to securely keep a copy all passwords.
5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection legislation (including GDPR).
 - This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
 - Any data being removed from the school site (such as via email or on memory sticks) will be suitably protected. 'Memory sticks' must be provided by the school and encrypted. School will need to securely keep a copy of the password.
 - Any images or videos of pupils will only be used as stated in the school image use policy and will always reflect parental consent.
7. I will not keep documents which contain school-related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use 'Cloud storage' (such as OneDrive or Google Drive) to upload any work documents and files in a password protected environment.

8. I will not store any personal information, such as personal photographs, files or financial information, unrelated to school activities, on the school computer systems including any school laptop or similar device issued to members of staff.

9. I will respect copyright and intellectual property rights.

10. I have read and understood the school's online safety policy which covers the requirements for use of mobile phones and personal devices and safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of learners within the classroom and other working spaces.

11. I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the Designated Safeguarding Lead (Paul Batchelor).

12. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, I will report this to the Head Teacher (or the Administration office) soon as possible.

13. My electronic communications with current or past pupils, parents/carers and other professionals will take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.

- All communication will take place via school approved communication channels, such as a school provided email address or telephone number, and not via my personal devices or communication channels, such as personal email, social networking or mobile phones.
- I will abide by the requirements for remote teaching as outlined in Annex C of Keeping Children Safe in Education, and the school policy "Remote Teaching and Learning."
- Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead (Paul Batchelor) and/or Head Teacher.

14. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming and any other devices or websites.

- I will take appropriate steps to protect myself online and will ensure that my use of IT and the internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school's Staff Code of Conduct and the Law.

15. I will not create, transmit, display, publish or forward any material online that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

16. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

17. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Designated Safeguarding Lead (Paul Batchelor) and/or the Head Teacher.

18. I understand that my use of the school information systems, including any devices provided by the school, including the school internet and school email, may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

19. I understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance. Where it

believes unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour may be taking place, the school may invoke its disciplinary procedures. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

(The acknowledgement slip will be circulated separately.)



North Nibley Church of England Primary School

Social Media Policy

Policy status	Required by Keeping Children Safe in Education (KCSiE) 2020
Responsible for this policy	Finance & Resources Committee (F&R)
Policy reviewed/amended	January 2021
Policy review frequency	Every 3 years
Policy due for renew	January 2024

North Nibley Church of England Voluntary Aided Primary School, formerly the William Purnell Endowed School, was founded in the Eighteenth Century to provide education for the children of North Nibley and the surrounding villages.

Our Vision is to inspire and celebrate learning, achievement, faith and fun.

Ours is a school that works in partnership with the community to enable and equip each child to “live life to the full” (The Gospel of John, Chapter 10 Verse 10), reflecting the Christian values of our foundation.

We will realise our Vision by:

- demonstrating, as a Church school, our Christian values in action
- providing a happy, healthy and secure environment where all are respected, valued and encouraged to contribute
- encouraging participation and a love of learning by offering experiences full of opportunity and creativity
- pursuing excellence in every aspect of school life, supporting one another and celebrating the achievements of all

This policy supports our vision by making clear that we, the staff, have a special responsibility to maintain and exemplify the highest standards of behaviour, encouraging our pupils by being role models on which children may pattern their lives. Our conduct, in person and online, should not bring teaching, our school or our community into disrespect. In making clear the boundaries within which we work, we also protect our own interests and thus enable all to flourish.

A Biblical Perspective: Titus Chapter 2, verse 7

“In everything, set them an example by doing what is good. In your teaching show integrity, seriousness.”

1. Introduction

The school recognises and embraces the numerous benefits and opportunities that social media offers. While employees are encouraged to engage, collaborate and innovate through social media, they should also be aware that there are some associated risks, especially around issues of safeguarding, bullying and personal reputation.

2. Purpose of the policy

2.1 The purpose of this policy is to encourage good practice, to protect the school and its employees, and to promote the effective use of social media as part of the school activities.

2.2 This policy covers personal and professional use of social media and aims to encourage its safe use by the school and its employees.

2.3 The policy applies regardless of whether the social media is accessed using the school's IT facilities and equipment, or equipment belonging to members of staff.

2.4 Personal communications via social media accounts that are likely to have a negative impact on professional standards or the school's reputation are within the scope of this policy.

2.5 This policy covers all individuals working at all levels and grades, including full-time and part-time employees, fixed-term employees and agency workers.

3. Roles, responsibilities and procedure

3.1 Employees should:

- be aware of their online reputation and recognise that their online activity can be seen by others including parents, pupils and colleagues on social media
- ensure that any use of social media is carried out in line with this policy and other relevant policies, ie those of the employer
- be aware that any excessive use of social media in school/college may result in disciplinary action
- be responsible for their words and actions in an online environment. They are therefore advised to consider whether any comment, photograph or video that they are about to post on a social networking site is something that they want pupils, colleagues, other employees of the trust, or even future employers, to read. If in doubt, don't post it!

3.2 Managers are responsible for:

- addressing any concerns and/or questions employees may have on the use of social media
- operating within the boundaries of this policy and ensuring that all staff understand the standards of behaviour expected of them.

3.3 Human resources (HR) is responsible for:

- giving specialist advice on the use of social media

4. Definition of social media

4.1 Social media is a broad term for any kind of online platform which enables people to directly interact with each other. It allows people to share information, ideas and views. Examples of social media include blogs, Facebook, LinkedIn, Twitter, Google+, Instagram, Myspace, Flickr and YouTube.

5. Acceptable use

5.1 Employees should be aware that content uploaded to social media is not private. Even if you restrict it to 'friends', there is still capacity for it to be re-posted or distributed beyond the intended recipients. Therefore, employees using social media should conduct themselves with professionalism and respect.

5.2 Employees should not upload any content on to social media sites that:

- is confidential to the school or its staff
- amounts to bullying
- amounts to unlawful discrimination, harassment or victimisation
- brings the school into disrepute
- contains lewd, sexually explicit, threatening or similarly inappropriate or offensive comments, images or video clips
- undermines the reputation of the school and/or individuals
- is defamatory or knowingly false
- breaches copyright
- is in any other way unlawful.

5.3 Employees should be aware of both professional and social boundaries and should not therefore accept or invite 'friend' requests from pupils or ex-pupils under the age of 18, or from parents on their personal social media accounts such as Facebook. All communication with parents via social media should be through the school's social media accounts.

5.4 Employees should note that the use of social media accounts during lesson time is not permitted.

6. Safeguarding

6.1 The use of social networking sites introduces a range of potential safeguarding risks to children and young people.

Potential risks can include, but are not limited to:

- online bullying
- grooming, exploitation or stalking
- exposure to inappropriate material or hateful language
- encouraging violent behaviour, self-harm or risk taking.

In order to mitigate these risks, there are steps you can take to promote safety on line:

- You should not use any information in an attempt to locate or meet a child.
- Ensure that any messages, photos or information comply with existing policies.

Further advice can be found in the appendix below.

7. Reporting safeguarding concerns

7.1 Any content or online activity which raises a safeguarding concern must be reported to the lead safeguarding officer in the school.

7.2 Any online concerns should be reported as soon as identified as urgent steps may need to be taken to support the child.

7.3 With regard to personal safeguarding, you should report any harassment or abuse you receive online while using your work accounts.

8. Reporting, responding and recording cyberbullying incidents

8.1 Staff should never engage with cyberbullying incidents. If in the course of your employment with this school/trust, you discover a website containing inaccurate, inappropriate or inflammatory written material relating to you, or images of you which have been taken and/or which are being used without your permission, you should immediately report this to a senior manager at your school.

8.2 Staff should keep any records of the abuse such as text, emails, voicemail, website or social media. If appropriate, screen prints of messages or web pages could be taken and the time, date and address of site should be recorded.

9. Action by employer: inappropriate use of social media

9.1 Following a report of inappropriate use of social media, the senior manager will conduct a prompt investigation.

9.2 If in the course of the investigation, it is found that a pupil submitted the material to the website, that pupil will be disciplined in line with the school's behaviour policy.

9.3 The senior manager, where appropriate, will approach the website hosts to ensure the material is either amended or removed as a matter of urgency, ie within 24 hours. If the website requires the individual who is complaining to do so personally, the school will give their full support and assistance.

9.4 Checks will be carried out to ensure that the requested amendments or removals are made. If the website(s) does not co-operate, the senior manager will contact the internet service provider (ISP) as the ISP has the ability to block access to certain sites and, in exceptional circumstances, can close down a website.

9.5 If the material is threatening and/or intimidating, senior management will, with the member of staff's consent, report the matter to the police.

9.6 The member of staff will be offered full support and appropriate stress counselling.

10. Breaches of this policy

10.1 Any member of staff suspected of committing a breach of this policy (or if complaints are received about unacceptable use of social networking that has potentially breached this policy) will be investigated in accordance with the school's bullying or disciplinary procedure. The member of staff will be expected to co-operate with the school's investigation which may involve:

- handing over relevant passwords and login details
- printing a copy or obtaining a screenshot of the alleged unacceptable content
- determining that the responsibility or source of the content was in fact the member of staff.

10.2 The seriousness of the breach will be considered including the nature of the content, how long the content remained visible on the social media site, the potential for recirculation by others and the impact on the school or the individuals concerned.

10.3 Staff should be aware that actions online can be in breach of the harassment/IT/equality policies and any online breaches of these policies may also be treated as conduct issues in accordance with the disciplinary procedure.

10.4 If the outcome of an investigation leads to disciplinary action, the consequences will be dealt with in accordance with the appropriate procedures. Serious breaches could result in the dismissal of the employee.

10.5 Where conduct is considered to be unlawful, the school will report the matter to the police and other external agencies.

11. Monitoring and review

11.1 If the manager reasonably believes that an employee has breached this policy, from time to time the school will monitor or record communications that are sent or received from within the school's network.

11.2 This policy will be reviewed on a triannual basis and, in accordance with the following, on an as-and-when-required basis:

- legislative changes
- good practice guidance
- case law
- significant incidents reported.

11.3 This policy does not form part of any employee's contract of employment and may also, after consultation with the trade unions, be amended from time to time by the school.

12. Legislation

12.1 Acceptable use of social networking must comply with UK law. In applying this policy, the school will adhere to its rights, responsibilities and duties in accordance with the following:

- Regulation of Investigatory Powers Act 2000
- General Data Protection Regulations (GDPR) 2018
- The Human Rights Act 1998
- The Equality Act 2010
- The Defamation Act 2013

13. Conclusion

13.1 The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media – the principles set out in this policy must be followed irrespective of the medium. When using social media, staff should be aware of the potential impact on themselves and the employer, whether for work-related or personal use; whether during working hours or otherwise; or whether social media is accessed using the employer's equipment or using the employee's equipment.

Staff should use discretion and common sense when engaging in online communication. There are some general rules and best practice in the appendix which staff may find helpful.

Appendix - Responsible use of social media – guidance for staff

Remember that anything you post online is not really private. Below are some common sense guidelines and recommendations that staff are advised to follow to ensure responsible and safe use of social media.

- Do not add pupils as friends or contacts in your social media accounts.
- Follow this social media policy.
- Always maintain professional boundaries. Do not engage in discussion with pupils online unless through official school accounts.
- Think about the potential risks: professional boundaries of adding parents to your private social media accounts (refer to policy).
- Consider using an alternative name on sites like Facebook to make it harder for pupils to find you. For example, some members use their partner's surname online but their own surname in school.
- Never post anything that is offensive or aggressive, even if you are very angry or upset. It can easily be taken out of context.
- Remember humour is relative. For example, posting images and/or text about a recent stag or hen night may be deemed inappropriate. Likewise, a few 'lighthearted' comments and/or

images about colleagues or students may not be perceived as such by either subject(s) of the humour or the employer. The guiding rule is: if in doubt, don't post it.

- Make sure you regularly check and refresh your site page to ensure it is free of any inappropriate comments and/or images.
- If you are tagged in something in Facebook that you consider inappropriate, use the remove tag feature to untag yourself (for details on how to do this, refer to the Facebook help centre).
- Be cautious of accepting 'friend requests' from people you do not really know. Simply being a 'friend' of your own Facebook friend does not mean that they should automatically be given access to your information.
- Review your profile information and settings on Facebook, Twitter and other sites to ensure it is appropriate as it may be accessed by others such as colleagues, pupils, parents and potential employers.
- Check your privacy and security settings regularly, and keep your date of birth and home address to yourself. Identity theft is a growing crime and this kind of information could be used to gain access to your bank or credit card account.
- If you feel dissatisfied and wish to rant about teaching, politics and life in general, consider doing so anonymously, through a networking account or blog which cannot be attributed to you. Check that anything that you post does not identify you, your school, pupils or parents.
- Ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation.
- Never post any information which can be used to identify a pupil.
- Do not use social media in any way to attack or abuse colleagues or air any other internal grievances.
- Do not post derogatory, defamatory, offensive, harassing or discriminatory content.
- Do not engage in any conduct (using personal insults, obscenities) which would not be acceptable in the workplace.
- Do not use social media to 'whistleblow' – raise concerns through the proper channels which would entitle you to legal protection (Public Interest Disclosure Act 1998).

North Nibley C of E Primary School

SAFE AND ACCEPTABLE USE OF TECHNOLOGY – CLASS POSTER

Our school has provided computers, tablets, Internet access and other technologies to help you learn. These rules will keep everyone safe and help us be fair to others. You are responsible for your own behaviour when using technology, just as you are in a classroom or on the playground.

The Acceptable Use Policy for children in Classes 1 & 2 **(Reception, Years 1 and 2)**

- I must not bring any technology in to school without the school's permission
- I only use the internet when an adult is with me
- I will keep my full name, my home address, my phone number and passwords safe
- I only send messages online which are polite and friendly
- I will not work with another child's files without a member of staff's permission
- I know the school can see what I am doing online
- I always tell a member of staff if something online makes me feel unhappy or worried
- I know that I should ask permission before printing my work
- I Know how to put devices away carefully and properly
- I have read and talked about these rules with my parents/carers
- I know that if I do not follow the rules then school can stop me from joining in
- I can visit <http://www.thinkuknow.co.uk> to learn more about keeping safe online

By following these rules, we will make using technology a safe and rewarding experience for everybody.



With thanks to the School Council, February 2019.

North Nibley C of E Primary School

SAFE AND ACCEPTABLE USE OF TECHNOLOGY – CLASS POSTER

Our school has provided computers, tablets, Internet access and other technologies to help you learn. These rules will keep everyone safe and help us be fair to others. You are responsible for your own behaviour when using technology, just as you are in a classroom or on the playground.

The Acceptable Use Policy for children in Classes 3 & 4 **(Years 3, 4, 5 and 6)**

Safe

- I must not bring any technology in to school without the school's permission, including memory sticks, cameras and CD's. Phones must be handed in to the office
- I only use the internet when an adult is with me
- I keep all my personal information and passwords safe

Meeting

- I only send messages online which are polite and friendly, and only to people that a member of staff has approved
- I will not arrange to meet anyone without my parent or teacher's permission
- I will not enter Internet chat rooms, other than those created by the school

Acceptable

- I will not accept or open emails, messages, or files from people I don't know
- I know the school can see what I am doing online and can look at my files at any time
- We will never allow bullying (including 'cyber-bullying') in our school
- I will not work with another child's files without a member of staff's permission
- I will not violate copyright laws or license agreements, crediting sources if needed
- I will not knowingly view, send, or display offensive materials. (If this happens, don't panic, or cause a fuss - just turn the monitor off and then tell a member of staff)

Responsible

- I Know how to fetch and put devices away carefully and properly
- I know that I should ask permission before printing my work, and do my best to limit waste such as disk space or printing ink and paper

Tell

- I always tell a member of staff if something online makes me feel unhappy or worried
- I have read and talked about these rules with my parents/carers
- I know that anyone using school technology in an unsafe or unacceptable way will have their use of technology suspended
- I can visit <http://www.thinkuknow.co.uk> to learn more about keeping safe online



With thanks to the School Council, February 2019