School Social Networking

Acceptable Use Policy

Wheatley Hill Community Primary School

Author:	*Alan Scarr*
Head Teacher:	*Alan Scarr*
Chair Of Governors:	*Vikki Wynn*
Date Written:	*July 2022*
Adopted by Governing Body:	*July 2022*
Date for Review:	*July 2023*

Staff Social Networking Acceptable Use Policy

1. As part of the school's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the school's approach to Online safety (e-Safety). I am aware that Social Media streams including Facebook / Twitter are a public and global communication tool and that any content posted may reflect on the school, its reputation and services. I will not use the social media accounts to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.

2. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Designated Safeguarding Lead and/or the head teacher. The head teacher retains the right to remove or approve content posted on behalf of the school.

3. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation also including GDPR May 2018.

4. I will follow the school's policy regarding confidentiality and data protection(GDPR)/use of images. This means I will ensure that the school has written permission from parents/carers before using images or videos which include any members of the school community. Any images of pupils will be taken on school equipment, by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school. These will be for the sole purpose of inclusion on social media and will not be forwarded to any other person or organisation.

5. I will promote online safety (e-Safety) in the use of Facebook / Twitter and will help to develop a responsible attitude to safety online and to the content that is accessed or created. I will ensure that the communication has been appropriately risk assessed and approved by a member of senior leadership team/ Designated Safeguarding Lead/head teacher prior to use.

6. I will set up a specific account/profile using a school provided email address to administrate the account/site/page and I will use a strong password to secure the account. Personal social networking accounts or email addresses are not to be used. The school Designated Safeguarding Lead and/or school leadership team/head teacher will have full admin rights to the site/page/group.

7. Where it believes unauthorised and/or inappropriate use of the account or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.

8. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.

9. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the head teacher and/or Designated Safeguarding Lead and/or Data Protection Officer urgently.

10. I will ensure that the site/page is moderated on a regular basis as agreed with the school Designated Safeguarding Lead.

11. I have read and understood the school Online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices and the safe use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the head teacher.

12. If I have any queries or questions regarding safe and acceptable practise online I will raise them with the Designated Safeguarding Lead or the head teacher.

I have read and understood and agree to comply with the School Social Networking Acceptable Use policy.

Signed: ……... Print Name: …… Date: ……

(Electronic Signatures May be Used Instead

Staff ICT Acceptable Use Policy

Wheatley Hill Community Primary School

Author: *Alan Scarr*	
Head Teacher: *Alan Scarr*	
Chair Of Governors: *Jayne Dinsdale*	
Date Written: *July 2022*	
Adopted by Governing Body: *July 2022*	
Date for Review: *July 2023*	

Staff ICT Acceptable Use Policy

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

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

1) I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include 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) Mobile Phones - The school outlines the use of mobile phones within the Staff Handbook and within the Online Safety Policy.

    a) Staff mobile phones are allowed in school, but are not allowed to be used in sensitive areas (EYFS, cloak rooms, toilets, when children are changing, swimming) nor should they be visible in public areas (corridors, dinner hall etc). Throughout contact time phones should be securely stored in staff lockers. Mobile phones should only be used for communication when not working with children and in a designated "Mobile Safe" zone. As outlined in the staff handbook, some members of staff may carry mobile phones throughout the day in order to maintain emergency communication links with educational visits, however these will remain concealed from children and set to silent / vibrate.

    b) Cameras on personal phones or tablets will not be used to take pictures of children in any circumstances.

    c) In the unlikely event of needing to contact a parent directly a school mobile phone will be issued to the member of staff concerned.

4) I understand that any hardware and software provided by my school for staff use can only be used by members of staff.

5) Personal use of school ICT systems and connectivity is only permitted when children are not present.

6) 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.

7) I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (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).

8) I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

9) Data Protection – GDPR Procedures and Policies – May 2018

   a) I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988 / GDPR May 2018. 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 (only within countries or sites with suitable data protection controls) or accessed remotely. Any personal data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school.

   b) If I choose to use a portable device (Phone, Tablet etc…) to collect my work e-mail I will ensure that the device is locked by a pin code or password and will be wiped when I dispose of the device.

   c) I will not transfer sensitive personal information from my school e-mail account (e.g. SEND plans, Safeguarding Reports, Medical Information) UNLESS the information is encrypted.

   d) Digital Images or videos of pupils will be only taken from the school premises using encrypted memory OR alternative secure transport method.

   e) I will not use unapproved cloud storage systems (Dropbox, icloud etc) for storing personal data of staff or pupils.

10) I will respect copyright and intellectual property rights.

11) Social Media.

   a) I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media.

   b) I will not communicate with pupils or ex-pupils under the age of 18 using social media without the express permission of the Headteacher.

   c) My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team. *This would include any relatives of current pupils that are my "friends" on a social media site.*

   d) My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

   e) I will not create, transmit, display, publish or forward any material 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. This would include any comment made, even in the belief that it is private on social media.

12) I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator Alan Scarr as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Alan Scarr as soon as possible.

13) 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, then I will report this to the ICT Support Provider/Team (ITSS) as soon as possible.

14) I will promote e-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.

15) If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-Safety Coordinator Alan Scarr - Head Teacher.

16) I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

ICT Agreements

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy – Updated July 2022. I fully understood the expectations of school GDPR and have been directed to the appropriate policies as required.

Signed: ……... Print Name: …… Date: ……

(Electronic Signature may be used via PeopleHR)

Staff Privacy Notice

Wheatley Hill Community Primary School

Author:	*Alan Scarr*
Head Teacher:	*Alan Scarr*
Chair Of Governors:	*Jayne Dinsdale*
Date Written:	*July 2022*
Adopted by Governing Body:	*July 2022*
Date for Review:	*July 2023*

Privacy Notice For Staff Members

This privacy notice explains how we collect, store and use personal data about staff members. We, Wheatley Hill Primary & Nursery School, are the ‘data controller’ for the purposes of data protection law.

Our data protection officer is Mrs Laura White.

Who we are and what we do

We are Wheatley Hill Primary & Nursery School, Wheatley Hill, Durham, DH6 3RQ. We are a maintained primary school for children ages 2 – 11 years old. Our local authority is Durham County Council.

The personal data we collect and hold

We hold personal data about staff to support their employment and professional development, and to assess how the school is performing. We may also receive data about staff from previous employers, HR and occupational health workers.

Personal data that we may collect, use, store and share (when appropriate) about staff includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Professional development records
- Bank details
- Maternity/paternity pay information
- Health information
- Performance management documentation
- Characteristics, such as ethnic background, disability etc
- Sickness absence records
- Details of any professional support received
- Photographs/videos

Why we use this data

We use this data to:

- Support you in your professional roles
- Monitor and report on school improvement and self-evaluation
- Provide appropriate pastoral care
- Protect pupil welfare
- Ensure that the information we hold about you is kept up to date
- To share with agencies such as payroll and pensions

Our legal basis for using this data

We collect and use personal data on the basis of performing a public task (educating children).

On some occasions we may ask for consent to process data when its use is optional. On those occasions consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Collecting this information

We collect data from application forms, paper forms, online information, communication with yourself, information received from a third party (eg. referees, colleagues, agencies)

How we store this data

We keep personal information about staff while they are working at our school. We may also keep it beyond their time at our school if this is necessary in order to comply with our legal obligations.

We will only retain the data we collect for as long as is necessary. This would be to satisfy the purpose for which it has been collected in accordance with our data retention policy. Please contact us if you would like further details on this policy.

The security of data and information is important to us. This is why we follow a range of security policies and procedures to control and safeguard access to and use of your personal information. This includes both physical and technical security and integrity of all data.

Examples of our security include:

- Encryption, meaning that information is hidden so that it cannot be read without access knowledge (such as a password). This is done with a secret code or what's called a 'cypher'. The hidden information is said to then be 'encrypted';
- Controlling access to systems and networks allows us to stop people who are not allowed to view your personal information from getting access to it;
- Training for our staff allows us to make them aware of how to handle information and how and when to report when something goes wrong;
- Regular testing of our technology and ways of working including keeping up to date on the latest security updates (commonly called patches);

How long we keep your data for
This ranges from months for some records to decades for more sensitive records.

For example

- applications for recruitment will be kept for 1 year,
- your personnel record will be maintained for 25 years after you leave employment

Data sharing
We may share your personal information where we have a statutory obligation to do so, such as for the purposes of the prevention or detection of crime, for legal proceedings, or where you have requested us to share information, such as childcare vouchers, pensions, mortgage applications etc.

Some examples of who we share information with include:-
HMRC (Her Majesty's Revenue & Customs)
DBS (Disclosure & Barring Service)
Pensions schemes
If you would like confirmation of who we do share information with please contact us.
We do not process your personal information outside the EEC.
At no time will your information be passed to organisations external to us, or our partners for marketing or sales purposes, or for any other commercial use without your prior express consent.

Your information rights

Your Information Rights are set out in the law. Subject to some legal exceptions, you have the right to:

- Have any inaccuracies corrected;
- Have your personal data erased;
- Place a restriction on our processing of your data;
- Object to processing; and
- Request your data to be ported (data portability).

To learn more about these rights please see the ICO website.

To exercise any of these rights please contact the relevant service in the first instance.

You also have the right to request a copy of the personal information that the school holds about you. To do this, please ask the DPO / Headteacher (AS)
If something goes wrong with your personal information, or you have questions about how we use it, please contact the Data Protection Officer / Headteacher (AS).

If we have not been able to deal with your complaint, you can also contact the Information Commissioner's Office

Information Commissioner's Office
Wycliffe House,
Water Lane
Wilmslow, Cheshire SK9 5AF

Other rights

Individuals have rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer:

Alan Scarr

Data Protection Officer

Wheatley Hill Primary & Nursery School

Wheatley Hill

Durham

DH6 3RQ

Tel: 01429 820594