Learning and living as children of God

(Ephesians 5:1)(You are God's children whom he loves. Try to be like God)

Staff Acceptable User Policy

September 2024

Computer network

- Obtaining, downloading, sending, printing, displaying, distributing or otherwise transmitting or gaining access to materials which are pornographic, obscene, racist, unlawful, abusive, offensive or inappropriate will be regarded as gross misconduct and will result in disciplinary action.
- Distributing abusive, discriminatory or defamatory statements will be regarded as gross misconduct and will lead to disciplinary action.
- You are responsible for the security of your passwords.
- The network must not be used for commercial purposes, e.g. buying or selling goods.
- No software is to be installed unless first agreed by Senior member of staff or appropriate IT representative to make sure that it is safe and has been properly Virus checked "
- Copyright of materials available on the network must be respected.

Internet / Email

- Use of GCC Internet and email must be solely for legitimate school purposes.
- Use of the internet and email are subject to scrutiny by the school's filtering provider. Any action that might damage the good reputation of the service will be dealt with as a serious act of misconduct.
- Use of the internet for personal financial gain, gambling, political purposes or advertising is forbidden.
- Emails sent from school should contain the same professional levels of language and content as applied to letters or other media.
- You are responsible for the email you send and for any contacts you make that might result in inappropriate emails being received.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Appropriate security must be used or applied before confidential or sensitive information is sent via the internet or email.
- All staff should avoid contacting students on social networking sites.This is to avoid any possible misinterpretation of motives and the risk of any allegations being made. Students must not be added to social media sites for staff.

Use of photographs, video and digital images

- Staff **must** only use school equipment to record, or take photographs of pupils, and only then if the relevant permission has been obtained. Please also see the GDPR policy.

Mobile Phones

- Professional tone to be used in all phone calls made and text messages sent using work phones.
- Personal calls, other than in an emergency, are forbidden on work phones.
- Calls and contact to pupils and parents should be restricted to the reasonable hours and only using school telephones or mobile telephones. Staff must not share their personal contact details.
- Direct contact with pupils by telephone calls or text messages should not happen

Remote education

Remote education, virtual lessons and live streaming KCSIE 2021

- Case studies on remote education practice are available for schools to learn from each other
- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely
- London Grid for Learning guidance, including platform specific advice
- National cyber security centre guidance on choosing, configuring and deploying video conferencing
- National cyber security centre guidance on how to set up and use video conferencing
- UK Safer Internet Centre guidance on safe remote learning

Social Media

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. (For detailed explanations please see the School Safeguarding Policy)

- Staff members **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.

- Staff members **must not 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 **must not to 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.

- If staff members need to communicate with pupils for work purposes they can only do so through the official school email or school mobile 'phone. Personal email addresses/phone numbers **must not** be shared with pupils or parents.

- 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.

- On leaving school employment, staff members **must not** 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.

- **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.

  - Staff members **are advised to set the privacy levels of their personal social media sites as strictly as they can** and to opt out of public listings on social networking sites 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)*

Filtering and monitoring

Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

The governors and staff in school will monitor the safe use of IT by carrying out regular filtering and monitoring checks. These are recorded for checking. All staff have been trained in cyber safety training.

Artificial Intelligence

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Deerhurst and Apperley Primary School recognises that AI has many uses, including enhancing teaching and learning, and in helping to protect and safeguard pupils. However, AI may also have the potential to facilitate abuse (e.g. bullying and grooming) and/or expose pupils to harmful content. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Deerhurst and Apperley Primary School will treat any use of AI to access harmful content or bully pupils in line with this policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out risk assessments for any new AI tool being used by the school.

BREACHES OF THE POLICY

- Any breach of this policy may be investigated and may lead to disciplinary action being taken against the staff member/s involved in line with School Disciplinary Policy and Procedure.

- A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of the school or any illegal acts or acts that render the school or the County Council liable to third parties may result in disciplinary action or dismissal.
- Contracted providers of the school must inform the relevant service or County Council officer immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the service and the County Council. Any action against breaches should be according to contractors' internal disciplinary procedures.

If you are in doubt about any of the above, please seek advice.

Please also read updated KCSIE 2024

Presented to Full Governing Body and agreed 8th October 2024

Signed: Head teacher Jayne Neveu Date

Signed: Chair of Governors Andrew Matthews Date

I have read and accept the terms of the:-

ICT, Technology and Social Media Acceptable Use 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: ______________________________