PRESTON & WINGHAM PRIMARY SCHOOLS FEDERATION

Acceptable Use Policy

What is an Acceptable Use Policy?

The Preston & Wingham Primary Schools Federation encourages and supports the positive use of Information and Communication Technology (ICT) to develop curriculum and learning opportunities as well as promoting personal enjoyment and achievements for all members of the community. It is essential that the use of ICT and online tools are carefully managed by the federation to ensure that all members of the community (including their data) are kept safe and that online risks and dangers are recognised and mitigated. The Acceptable Use Policy (AUP) is an integral and essential part of this process.

The AUP will be reviewed regularly by the governing body to ensure that it remains appropriate to the needs and the requirements of the federation. The AUP will be revisited and updated in response to any changes, for example after an incident, introduction of new technologies or after any significant changes to the school organisation or technical infrastructure. Any amendments to the AUP will be communicated and shared with all members of the community.

The AUP is a crucial tool for senior leaders to identify and establish online safety as part of the whole school safeguarding culture and covers the requirements as identified within keeping children safe in education 2016. It focuses on the behaviours rather than the technology itself and has been adapted according to the federation’s own approaches and ethos. The AUP should be considered alongside other federation policies that are in place in order to keep children safe e.g. the staff handbook, safeguarding policy, behaviour policy etc.

The AUP is not intended to unduly limit the ways in which members of staff teach or use ICT personally or professionally, but aims to ensure that the federation and all members of staff comply with the appropriate legal responsibilities, the reputation of the federation is maintained and the safety of all users is ensured. With internet use becoming more prominent in everyday life for both personal and professional use, it is important that all members of staff are aware that their online conduct both in and out of school could have an impact on their role and reputation. Civil, legal or disciplinary action could be taken should they be found to have brought the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities. All adults who work within the federation either as employees or volunteers must be aware of the federation rules and expectations for use of school information systems and professional conduct online whether on or off site. Misuse of ICT systems and other professional misconduct rules for employees (whether from Kent County Council or other professional bodies) are specific and instances resulting in disciplinary procedures or staff dismissal have occurred.

Acceptable Use by Pupils

Through Computing lessons and the wider curriculum all pupils will be taught:

- to only use the internet when an adult is present
- to only click on links and buttons when they know what they do
- to keep their personal information and passwords safe online
- to only send messages online which are polite and friendly
- that the school can see what they are doing online at all times
- If they see anything online that they shouldn't or that makes them feel worried or upset then they will minimise the page and tell an adult straight away
- that they can visit www.thinkuknow.co.uk (include other appropriate links) to learn more about keeping safe online
- to know that not everything or everyone online is honest or truthful
- that they must not access or change other peoples files or information
- that they can only change the settings on the computer if a teacher/technician has allowed me to
- that people they meet online may not always be who they say they are. If someone online suggests meeting up, they must immediately talk to an adult
- that If they are aware of anyone being unsafe with technology then they will report it to a teacher

Letter for Staff

Dear Colleague,

Social media can blur the definitions of personal and working lives, so it is important that all members of staff take precautions in order to protect themselves both professionally and personally online.

- Be very conscious of both your professional reputation and that of the school when you are online.
- All members of staff are strongly advised, in their own interests, to take steps to ensure that their personal information and content is not accessible to anybody who does not or should not have permission to access it.
- All staff must also be mindful that any content shared online cannot be guaranteed to be “private” and could potentially be seen by unintended audiences which may have consequences including civil, legal and disciplinary action being taken.
- Ensure that your privacy settings are set appropriately (many sites have a variety of options to choose from which change regularly and may be different on different devices) as it could lead to your content accidentally being shared with others.
- Be very careful when publishing any information, personal contact details, video or images etc online; ask yourself if you would feel comfortable about a current or prospective employer, colleague, child in your care or parent/carer, viewing or sharing your content. If the answer is no, then consider if it should be posted online at all. It is very important to be aware that sometimes content shared online, even in jest, can be misread, misinterpreted or taken out of context, which can lead to complaints or allegations being made. Don’t be afraid to be yourself online but do so respectfully. All staff must be aware that as professionals, we must be cautious to ensure that the content we post online does not bring the school or our professional role into disrepute.
- If you have a social networking account, it is advised that you do not to accept pupils (past or present) or their parents/carers as “friends” on a personal account. You may be giving them access to your personal information and allowing them to contact you inappropriately through unregulated channels. They may also be giving you access to their personal information and activities which could cause safeguarding concerns.
- Please use your work provided email address or phone number to contact children and/or parents – this is essential in order to protect yourself as well as the wider community. If you have a pre-existing relationship with a child or parent/carer that may compromise this or have any queries or concerns about this then please speak to me.

I would like to remind all staff of our Acceptable Use Policy and the importance of maintaining professional boundaries online. Failure to follow this guidance and the school policy could lead to disciplinary action, so it is crucial that all staff understand how to protect themselves online. Please speak to the Head of School or myself if you have any queries or concerns regarding this.

Yours sincerely,

Executive Headteacher

PRESTON & WINGHAM PRIMARY SCHOOLS FEDERATION

Staff 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 ethos of the federation, other appropriate federation/school policies, relevant national and local guidance and expectations, 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 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.
4. 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 and is changed regularly).
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 Act 1998. 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 that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any 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. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.
7. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted. Where possible I will use the School Learning Platform to upload any work documents and files in a password protected environment (if appropriate) or via VPN. I will protect the devices in my care from unapproved access or theft.

8. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.
9. I will respect copyright and intellectual property rights.
10. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.
11. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Safeguarding Lead as soon as possible.
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, then I will report this to the Executive Headteacher and Head of School as soon as possible.
13. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels eg. via a school provided email address or telephone number and not via personal devices or communication channels eg. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Executive Headteacher.
14. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.
15. 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 dispute.
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, then I will raise them with the Designated Safeguarding Lead.
18. Schools will need to include specific details and expectations regarding safe practice relating to the specific use of technology within school eg. tablets etc.
19. I understand that my use of the school information systems (including any devices provided by the school), 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. *The School may exercise its right to monitor the use of information systems, including Internet access and the interception of emails in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use of the schools information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the school suspects that the school system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.*

20. I will ensure that volunteers/visitors to the school do not use the school's computing equipment or systems unless accompanied by a member of staff.

I have read and understood and agree to comply with the Staff Acceptable Use Policy.

Signed: ………………………..... Print Name: ……………………… Date: ……… Accepted by: ……………………………. Print Name: …………………………

Wi-FiAcceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the schools boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. This is not an exhaustive list and all members of the school community are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

Please be aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The School takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the School premises that is not the property of the School.

The school provides Wi-Fi for the school community and allows access for education use only.

1. The use of ICT devices falls under The Preston & Wingham Primary Schools Federation Acceptable Use Policy, online safety (e-Safety) policy, safeguarding policy and behaviour policy which all members of the school community must comply with.
2. School owned information systems, including Wi-Fi, must be used lawfully and 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 will take all practical steps necessary to make sure that any equipment connected to the schools service is adequately secure (such as up-to-date anti-virus software, systems updates).
4. The school accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the school's wireless service's connection to the Internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other Internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.
5. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service. I will respect system security and I will not disclose any password or security information that is given to me. 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.
6. I will not attempt to bypass any of the schools security and filtering systems or download any unauthorised software or applications.
7. My use of the school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
8. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.
9. I will report any online safety (e-Safety) concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead as soon as possible.
10. If I have any queries or questions regarding safe behaviour online then I will discuss them with the Executive Head Teacher.

11. I understand that my use of the schools Wi-Fi will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the schools suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school terminate or restrict usage. If the School suspects that the system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with (name) school Wi-Fi Acceptable Use Policy.

Signed: ………………………..... Print Name: ……………………… Date: ………

Accepted by: ……………………………. Print Name: ………………………….

Case Studies

Kent Schools and Settings are invited to share their examples of approaches to developing AUPs with students, staff and parents/carers with the Education Safeguarding Adviser (Online Protection) or the e-Safety Development Officer. Examples will be added to the document and e-Safety blog to share good practice with others.

The Judd School

"Our existing policy was original written over 20 year ago and although it had been updated over the years it had reached the point where it needed to be "retired". My first point of call was the Kent website because I knew there was a staff ICT policy template.

As the network manager I had performed the first edit of the document using the KCC Template. What I wanted to achieve was an A4 document – too many statements and I felt the students would "switch off". The first step was to group the statements under responsibility, e-safety (staying safe on-line) and having a positive digital footprint and I removed any statements that were repetitive. Next I added one or two statements from our original policy as students must understand that the school network (including computers) should be treated with respect too.

I took the first draft to a group of sixth formers and they seemed happy with the fact that there is a need for an ICT policy and didn't suggest any changes. The next step was to share the AUP with our staff e-safety group who added additional content about not playing computer games unless given permission by a member of staff (we are a boys school) and also changed the order of the sections as they felt that the positive statements (e-safety and digital footprint) should come first and the responsibility statements should come last. We then added the reminder for the ThinkUKnow site should students need help and support.

The next stage is to obtain approval from our Governors. Once approved students will need to agree to this policy when they next log onto a school computer. I will ask that form tutors read through the statements with their form members plus a copy will be sent home to parents."

Acknowledgements and Thanks

This document and statements have been produced with thanks to members of Kent County Council Online safety (e-Safety) Strategy Group and material from Plymouth County Council, UK Safer Internet Centre, South West Grid for Learning, Childnet International and CEOP. Also thanks to The Judd School, Kingsnorth Primary School. Loose Primary School, Peter Banbury, Kent Police, Kent Schools Personnel Service (SPS), Kent Legal Services, Kent Libraries and Archives, KCC ICT and EiS Kent for providing comments, feedback and support.