Acceptable Use Policies for Educational Settings

November 2018

THE EDUCATION PEOPLE

Contents

Acceptable Use Policies for Educational Settings

Leaders and managers within education settings will be encouraging and supporting the positive use of technology for all members of their communities to develop curriculum and learning opportunities, as well as for personal enjoyment and achievement. The use of technology and the internet will need to be carefully managed to ensure that all members of the community are kept safe; Acceptable Use Policies (AUPs) are an integral part of this process.

What is an AUP?

AUPs are a crucial tool for managers and leaders to help identify and establish online safety approaches. An AUP:

- Is a clear and concise document which gives all users an outline of acceptable and unacceptable behaviours
- should focus on behaviours rather than technology itself
- Should be developed with end-user input to engage and empower all members of the community
- Is appropriate to the settings needs and requirements; settings will need different versions for different audiences within the community
- Is embedded as part of staff induction and new learner intake
- Is developed by the Designated Safeguarding Lead (DSL) as part of leadership and management and is approved by the Governing Body or trust/committee, as appropriate.
- Encourages all members of the community to develop responsibility for their behaviour and practice online, as appropriate
- Clearly states what monitoring takes place on ICT systems on site, or via devices provided by the setting
- Outlines the sanctions for unacceptable use
- Should be clear about what someone should do if they become aware of a potential breach of the AUP or are concern or unsure
- Signposts users to named contacts within the setting for support or questions
- Must be monitored, reviewed and updated regularly by senior leaders/managers

AUPs should be developed by a member of leadership and/or management, and should be approved by the headteacher, manager, and Governing Body/Trust, as appropriate.

Guidance for use

This document has been written by the Education People's Education Safeguarding Service with input from children and education professionals. It includes guidance and templates to help leaders and managers within educational settings develop appropriate Acceptable Use Policies (AUPs) and make informed decision reading their development and application.

This document has been developed for all educational settings including (but not limited to) schools, early year's settings, colleges, Pupil Referral Units, 14-19 settings, alternative curriculum provisions and hospital schools. For simplicity we have used the terms 'school' and 'pupils' or 'students' within this document, but stress that its use within other educational settings and beyond, are relevant and appropriate.

Elements in the AUP template highlighted in red are areas where educational settings should personalise the template. Content in blue will require settings to make informed leadership decisions and add or amend content accordingly. We encourage all settings to ensure that their AUP is fit for purpose and individualised for their context; including technology use and specific community needs. Not all templates or statements within the guidance will be required for all settings.

Educational settings should work in partnership with their stakeholders to ensure that the AUP is adapted appropriately; this will ensure that all members of the community have clear understanding, awareness and 'ownership' of the AUP.

Keeping up-to-date

AUPs should be reviewed at least annually, to ensure they are appropriate to the settings needs and requirements. AUPs should also be revisited and updated in response to any changes, for example after an incident, following any changes to local and/or national guidance, introduction of new technologies to the setting or after any significant changes to the organisational or technical infrastructure. Any amendments to the AUP should be communicated and shared with all members of the community.

Due to the constantly evolving nature of technology and updates to local and national guidance and legislation, this document may be updated frequently. Educational leaders can subscribe to the online safety blog for updates.

Questions and queries

If Kent education settings wish to discuss this document or any other online safety concerns, contact the Education Safeguarding Advisor (Online Protection) or Online Safety Development Officer.

Additional resources and materials

Kent Resources

- The Kent online safety materials for educational settings can be found at: www.theeducationpeople.org and www.kelsi.org.uk/child-protection-and-safeguarding/e-safety
- Kent educational settings can consult with the Education Safeguarding Service; specific advice is available via the Education Safeguarding Advisor (Online Protection) and Online Safety Development Officer
- Centralised online safety training for Designated Safeguarding Leads within education settings is available via CPD Online.
- "Safe Professional Practice with Technology" is a Kent Safeguarding Children Board (KSCB) document which discusses ideas and FAQs for professionals on how to use technology safely when working with young people.

Other resources

- UK Safer Internet Centre: www.saferinternet.org.uk
    - The UK Safer Internet Centre's Professional Online Safety Helpline offers advice and guidance regarding online safety issues for professionals who work with children and young people in the UK. Staff can contact the helpline via 0844 381 4772 or helpline@saferinternet.org.uk.
- Think U Know: www.thinkuknow.co.uk
    - CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
- Childnet International: www.childnet.com
    - "Supporting School Staff" is a useful document to help staff understand how to protect themselves online created by Childnet
- Internet Matters: www.internetmatters.org
- 360 Degree Safe tool is an online audit tool for schools from the South West Grid for Learning (SWGfL) to review current practice
- Online Compass is an online safety self-review tool applicable for any organisation working with children, from early years to voluntary organisations; from youth clubs to work placement and allows organisers to assess their own online safety provision.

AUPs for Staff, Visitors and Volunteers

Why do educational settings need an AUP for staff?

Leaders, governing bodies and proprietors should be aware of the statutory duties and responsibilities placed upon educational settings within 'Keeping Children Safe in Education' (KCSIE) 2018.

KCSIE 2018 identifies that:

- *47. Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare.*
- *48. This should include:*
    - *a staff behaviour policy (sometimes called the code of conduct) which should amongst other things include - acceptable use of technologies, staff/pupil relationships and communications including the use of social media.*

It is essential that leaders, governing bodies and proprietors ensure that their settings have an appropriate AUP in place; either as a separate document or embedded within the staff behaviour policy or code of conduct.

When creating an AUP, educational settings should be mindful of a range of national guidance and legislation, including but not limited to:

- Teaching Standards
    - The preamble states that: "*Teachers make the education of their pupils their first concern and are accountable for achieving the highest possible standards in work **and conduct**. Teachers act with **honesty and integrity**; have strong subject knowledge, keep their knowledge and skills as teachers up-to-date and are self-critical; forge **positive professional relationships**; and work with parents in the best interests of their pupils*."

- 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' (2015)

- Health and Safety at Work Act 1974 and the Management of Health and Safety at Work Regulations 1999 places a duty of care on leaders and managers to safeguard and protect staff

- Children Act 2004, section 11 places a duty on key persons and bodies to ensure that their functions are discharged having regard to the need to safeguard and promote the welfare of children

- Data Protection Legislation, including General Data Protection Regulations (GDPR) and Data Protection Act 2018.
    - KCC Data Protection information is available on Kelsi and specific guidance for education establishments, including information on how to register and check notification can be found on the ICO website

Considerations for staff AUPs

Misuse of IT systems and other online professional misconduct rules for employees are specific; instances resulting in disciplinary procedures or staff dismissal have occurred. All adults who work within educational settings, either as employees or volunteers, including teaching, non-teaching staff, PTA groups, contractors and governors, should be made aware of the expectations for use of information systems and the importance of professional conduct online, whether on or off site.

Leaders and managers may wish to seek legal advice or access support from unions or personnel services to ensure their AUP is fit for purpose. Members of staff are entitled to seek their own legal advice before signing the AUP.

The AUP should form an essential part of the induction process for all staff, including visitors or volunteers who may have access to learners as well as school information and IT systems, or could be viewed as representing the setting.

Staff AUPs should:

- Apply to all staff within the setting
    - Learners could disclose concerns to any members of staff
    - All staff can be vulnerable to misuse or at risk of allegations
- Not unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally
- Ensure that the all members of staff comply with their appropriate legal and safeguarding responsibilities
- Ensure that the positive reputation of the setting is maintained
- Ensure the safety of all users is paramount

If concerns are raised by staff regarding the AUP, leaders and managers should discuss issues either directly with the member of staff concerned or the wider staff group, if applicable. In many cases staff members raise issues with AUPs when they are unclear or unhappy about the language or terminology used; this can sometimes be avoided by engaging with staff as part of the development process.

Professional reputation and social media

With internet use becoming more prominent in everyday life for both personal and professional use, it is important that all members of staff are made aware that their online

conduct both in and out of work 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.

Educational settings should be aware they cannot ban staff from using social media in their own personal time; however, they can and should provide advice to staff regarding boundaries relating to online communication and interaction with children and parents/carers, both current and past.

Although specific information should be covered within social media policies or staff training, AUPs may be helpful place to remind staff of the settings expectations. Some educational settings may wish to provide explicit guidance for staff, volunteers and visitors regarding the use of social media within the AUP as even when use of social media sites takes place in their own time using their own devices, it can leave staff vulnerable to abuse or a blurring of professional boundaries.

Many educational settings are now using social media as a communication or teaching and learning tool; if so, AUPs should be updated to reflect this use. Specific AUPs to reflect the official use of social media by staff and volunteers are included within this document and additional guidance regarding official use of social media is available via the Education People.

Communication with children and their families

Leaders and managers should make their expectations regarding online contact between staff and children explicitly clear as part of whole staff training and induction; all staff should ensure that any communication takes place within clear and explicit professional boundaries and is transparent and open to scrutiny.

It is recommended that any contact with learners and parents (past or present) takes place via work approved and provided communication channels, for example a setting email address or the learning platform. This means that communication can be monitored and traced in the case of an allegation or concern.

Educational settings should recognise that in some cases there may be pre-existing or external relationships which mean that a total “ban” on staff adding learners or their family members as friends or contacts on personal social networking sites may be difficult to enforce. This could include situations where such as where learners or their parents are family members of staff. Members of staff should be instructed to discuss these exceptions with the DSL to protect themselves from allegations or misinterpreted situations.

Use of setting systems and devices

Settings should be clear that any online behaviour and activity by a member of staff whilst using the work systems or devices must not interfere with the member of staff's duties or be for commercial purpose or gain, unless officially authorised by the leadership or management team.

Educational settings could also use the AUP to highlight their decision regarding staff using setting equipment for personal use. Occasional personal use of the settings devices could be considered as beneficial to the development of staff IT skills and can enable staff to maintain a positive work-life balance. However, this is at the setting's discretion and can be revoked at any time.

Monitoring

Staff must be made aware that any use of settings systems can be monitored; this is to safeguard systems from misuse, not to spy on staff's personal life. Staff should be reminded that it is their choice to use settings systems for personal use and that any monitoring takes place in accordance with relevant privacy legislation.

Leaders and managers should be aware that monitoring, seizing and searching members of staffs' personal devices may be unlawful. If leaders and managers feel this is required or appropriate, for example if they believe a criminal offence has been committed, the appropriate agency should be informed in line with child protection and/or allegations policies.

External contractors or service providers

Where the setting outsources services, such as IT, transport providers, maintenance or catering, an AUP for contracted staff should be created as part of the service level agreement. This AUP should be owned and enforced by both the managed service provider and the educational setting.

Some settings may believe that as contracted staff as not employed by the settings or do not access IT systems, an AUP is unnecessary. However, contracted staff may still interact with learners so could receive disclosures, they could accidently or intentionally share confidential information, or could be vulnerable to professional practice concerns or allegations if boundaries are not made clear. A clear AUP may help reduce these issues.

Visitors and volunteers

Whilst it won't be necessary for all visitors and volunteers to sign an AUP, it is important that educational settings provide regular visitors and volunteers with clear expectations regarding online behaviour and confidentially.

Visitors and volunteers who may need to sign an AUP (either an amended version of the staff AUP or potentially a separate document) include:

- Governors or trust/committee members
- Parent volunteers
- Visiting IT staff, such as mobile technicians
- External speakers or organisations working with learners

In some cases, visitor or volunteers may not have accessed any professional training regarding child protection or safe professional practice. AUPs can help ensure that clear information regarding the settings expectations relating to online conduct is provided; this is especially important to ensure confidentiality policies are respected. For example, a concern could arise if a parent volunteer posted comments on social media about another child's behaviour.

There will also be situations whereby visitors and volunteers may need to have access to or use settings systems and/or data, such as governors, visiting IT staff or external speakers. It is important that clear expectations are put in place regarding appropriate access and behaviour prior to access being permitted.

How should educational settings develop and implement an AUP for staff?

All members of staff, including visitors and volunteers, should be given time to read, understand and sign the AUP before being granted access to any of the settings IT systems. The AUP should be firmly embedded within the induction process for all members of staff, including volunteers, part-time staff or work experience placements.

Some educational settings may be able to display the AUP, or a reminder of core statements, at the point of access to IT systems; for example, when members of staff login to school systems or devices. Leader and managers should consider if they have the technical ability to implement this approach and be mindful of the limitations.

An AUP cannot be a substitute for up-to-date and relevant online safety training; this will help ensure that the thinking behind the AUP is understood and supported throughout the staff group.

It is strongly recommended that members of staff be actively involved in creating the AUP. This should include involving and inviting staff to contribute and express views and opinions during the creation and reviewing process. This will increase ownership of the AUP and enable settings to ensure that it is appropriate and reflects the needs and requirements of the establishment.

Acceptable Use Policies for Learners

Why do educational settings need an AUP for learners?

Educational settings have a duty of care to safeguard learners and take all reasonable steps to ensure that their internet use is lawful. As highlighted by Ofsted (Common Inspection Framework and the Inspecting Safeguarding document), it is essential that education settings support children in learning to manage online risks both at school and at home.

With internet use an essential feature of children and young people's everyday life, it is important that they are made aware that their online conduct both on and off site can have an impact within and outside of the setting. In some situations, criminal, civil or disciplinary action can be taken; depending upon the child's age and circumstances. It is therefore important that the AUP is supported with regular, embedded and progressive education for children, which clearly highlights safe and positive online behaviour, appropriate to their age and ability.

Considerations for AUPs for learners

Any online behaviour and/or activity should be in accordance with the settings AUP and behaviour policy, not interfere with the learners' education and comply with the law.

.

Learners AUPs should:

- Not unduly limit the ways in which learners use technology to learn, communicate, play or socialise
- Ensure that learners are aware of safe and appropriate online behaviour
- Ensure that the positive reputation of the setting is maintained
- Ensure learners are aware of sanctions for misuse
- Empower and support learners to take responsibility for their own use of technology
- Highlight how to report online safety concerns both internally and externally

Use of setting systems and devices

It is important that the AUP for learners reflects the use of specific systems or devices used within the setting, such as use of tablets and cameras. AUPs should include expectations for safe use of technology when using tools not fully under the settings control, or when using external systems such as cloud storage, email, and apps.

Settings may wish to add a statement regarding learners using setting equipment for personal use; occasional personal use can be beneficial to the development of IT skills. However, this can bring safeguarding concerns and risks; access should be at the settings discretion and can be revoked at any time. This approach should be carefully risk assessed

and appropriate safeguarding approaches such as filtering, monitoring and education must be in place.

Monitoring

Learners must be made aware, prior to access, that their internet and technology use may be recorded or monitored for safety and security reasons. Settings will need to consider how learners' activity can be captured or monitored, such as supervision or recording logins to devices, systems or wireless internet access.

If settings use additional monitoring products or systems to record the conduct of learners when using setting owned ICT systems, they must ensure they are explicitly made aware of this activity prior to access and that monitoring is in accordance with the law.

The UK safer internet centre has information for educational settings regarding appropriate filtering and monitoring.

Personal Devices and mobile phones

Educational settings may also want to consider adapting the AUP according to their own policy and procedures if they allow learners to use personal devices, such as mobile phones, on-site.

For further information regarding mobile phones and personal devices, settings should access the online safety policy template available via Kelsi.

How should educational settings develop and implement AUPs for learners?

The templates within this document provides a selection of possible statements for AUPs for learners; they will need to be adapted by settings according to their own online safety ethos and approach, as well considering their individual requirements and systems.

To protect learners, it is important to have an AUP in place which has been viewed and discussed in a way which is appropriate to their age and abilities. All learners who use IT must be aware of the settings expectations whether on or off site. Different versions of the AUP might be required as learners' transition through key stages, due to the changes in how children use and access technology as well as to reflect their ability to understand and manage their own behaviour.

The AUP should be presented in a format which is accessible to all learners, including those with special educational needs and disabilities. Settings may need to work with SENCOs and other specialist services to ensure that the AUP is accessible and understood by all members of the community.

Some educational settings could consider displaying the AUP, or a reminder of core statements, at the point of access to IT systems. For example, when learners' login to setting systems or devices, they could be prompted to read and confirm the AUP on screen before being able to access systems or the internet. Leader and managers should consider if they have the technical ability to implement this approach and be mindful of the limitations, for example if learners cannot read or understand the rules. It is likely that this approach will depend on the IT provision and resources available, as well as the age and ability of learners.

Whilst AUPs should be developed by a member of the leadership team and be approved by the headteacher/manager and Governing Body as appropriate; it is strongly recommended that learners should be actively involved in creating the AUP. This acknowledges the voice of learners within the setting and will help empower them to develop safe and appropriate online behaviour. Settings may wish to undertake this by involving pupil or student councils or could opt to have a wider engagement approach, for example as part of class or tutor discussions.

To be successful, the AUP needs to be included as part of an embedded and progressive online curriculum. The AUP should be discussed with learners on a regular basis as well as when they are using technology. The AUP may feature within specific online safety education but should not just be discussed in isolation, for example only within computing lessons. The AUP statements will need to be fully explored and discussed with learners to ensure that they understand the statements, are aware of the consequences and know how to access support.

How can educational settings engage with parents and carers?

Considerations

The AUP should be shared with parents and carers to develop a cohesive approach to online safety. It's important that parents and carers are aware of the settings online safety ethos and are actively engaged in supporting and delivering online messages. Settings should be using their AUP as a way of engaging families; this can help establish a shared responsibility and approach to online safety from the beginning.

Settings may wish to involve parents and carers in the development of AUPs for the community. This could be achieved by engaging directly with active and interested groups such as Parent Teacher associations or friend's associations. Alternatively, settings could canvas the entire parent/carer community by sharing AUPs with requests for comments or feedback. This approach may depend on the size and composition of the community.

Parents and carers will need to be made aware that the setting will take every effort and all reasonable precautions to ensure that children cannot access inappropriate or illegal content on site; however, this cannot always be possible due to the dynamic nature of the internet. Settings should reassure parents of the precautions they will take to limit this risk, such as the use of filtering and monitoring systems and supervision of children.

Home School Agreements

It is recommended that parental awareness and engagement with the AUP is achieved by including it as part of the Home School Agreement, which parents' usually access when children start attending the provision. Settings could also use the Home School agreement to ensure parents are aware of the expectations of online conduct for the whole community. Settings may wish to include specific statements such as: "*We are aware of the Acceptable Use Policy and will support the schools' approach to online safety. We, with our child will not upload, share or add any pictures, video or text that could upset, offend or threaten the safety of any member of the setting community*".

Permission

Many settings require children and parents/carers to return a slip to say they have read and understood the AUP. Settings will need to decide whether they wish parents to sign to acknowledge the AUP on behalf of, or alongside their child; this may depend on the age and ability of children.

Some settings will choose to obtain parents acknowledgement regarding AUPs on an annual basis, others at point of admission and/or transition between key stages; this may depend on the setting type and will need to be an administration and leadership decision.

For early years settings and infant schools, it is unlikely that children will be able to "sign" or give informed consent for an AUP, however, it is important that children are involved as much as is possible in this process as online safety education begins as soon as children begin using technology.

Some settings opt to request that parents and carers read **and** sign the AUP to give permission for children to use the internet and associated technologies; this is not the same as signing to acknowledge the AUP. This approach can cause problems as some parents may refuse to give consent for access or may simply not respond. Children will need to use the internet to access the curriculum and denial of access could impact learning. If settings decide to request parental consent for internet access, they will need to have a robust process in place to manage and record parental responses and engage with parents who do not respond or refuse consent.

Educational settings will need to decide which approach for parental engagement best suits their community; leaders and managers should carefully consider which approach would be the most applicable.

AUPs for Parents

Some settings require parents and carers to sign a specific AUP aimed at them to highlight how the setting and family will work together to keep the community safe online. The decision to take this approach may depend on settings specific use of technology with parents and carers, for example if formal communication channels such as apps to track or share data, email or text messages is utilised by parents and carers.

Some sample AUPs are included within this document for settings to adapt if this approach is preferred.

Learner Acceptable Use Policy: Sample Statements

The following statements are provided as suggestions and guidance only and it is recommended that settings write their own AUP to reflect the needs and abilities of their learners, community, the technology available and the settings online safety ethos. Where possible and appropriate, learners should be directly involved in this process.

Although the statements for learners are collected within key stages it is recommended that settings amend and adapt them according to their own cohorts as appropriate. Settings will need to adapt these templates in line with their own technology use, for example the expectations or requirements may vary if settings use laptops or tablets.

Larger versions of the posters available for use to reinforce the expectations regarding acceptable use of technology can be found on Kelsi.

Early Years and Key Stage 1 (0-6)

Possible Statements

- I only use the internet when an adult is with me
- I only click on links and buttons online when I know what they do
- I keep my personal information and passwords safe online
- I only send messages online which are polite and friendly
- I know the school can see what I am doing online
- Schools should include specific information and expectations relating to use of devices in school, for example tablets, cloud computing, pupil owned devices
- I know that if I do not follow the rules then:
    - List sanctions
- I have read and talked about these rules with my parents/carers
- I always tell an adult/teacher if something online makes me feel unhappy or worried
- I can visit www.thinkuknow.co.uk (include other appropriate links) to learn more about keeping safe online

Shortened version (for use on posters)

- I only go online with a grown up
- I am kind online
- I keep information about me safe online
- I tell a grown up if something online makes me unhappy or worried

Early Years and KS1 Acceptable Use Poster

Key Stage 2 (7-11)

Possible Statements

These headers are suggestions only; we encourage educational settings to work with children to amend them accordingly.

Safe

- I only send messages which are polite and friendly
- I will only post pictures or videos on the internet if they are appropriate and if I have permission
- I only talk with and open messages from people I know, and I only click on links if I know they are safe
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult

Trust

- I know that not everything or everyone online is honest or truthful
- I will check content on other sources like other websites, books or with a trusted adult
- I always credit the person or source that created any work, image or text I use

Responsible

- **Schools should include specific information and expectations relating to the use of devices and technology e.g. tablets, laptops, cloud computing, shared file storage areas.**
- I always ask permission from an adult before using the internet
- I only use websites and search engines that my teacher has chosen
- I use school computers for school work, unless I have permission otherwise
- I ask my teacher before using my own personal devices/mobile phone (**other specific statements will be required if mobile phones/personal devices are or are not permitted**)
- I keep my personal information safe and private online
- I will keep my passwords safe and not share them with anyone
- I will not access or change other people's files or information
- I will only change the settings on the computer if a teacher/technician has allowed me to

Understand

- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- I know that my use of school devices/computers and internet access will be monitored

- I have read and talked about these rules with my parents/carers
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about keeping safe online
- I know that if I do not follow the school rules then:
    - List sanctions

Tell

- If I am aware of anyone being unsafe with technology, I will report it to a teacher
- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened
- If I see anything online that I shouldn't or that makes me feel worried or upset then I will minimise the page and tell an adult straight away (**amend to reflect schools approach e.g. shut the laptop lid, turn off the screen**)

Alternative KS2 Statements *(With thanks to Kingsnorth Primary School)*

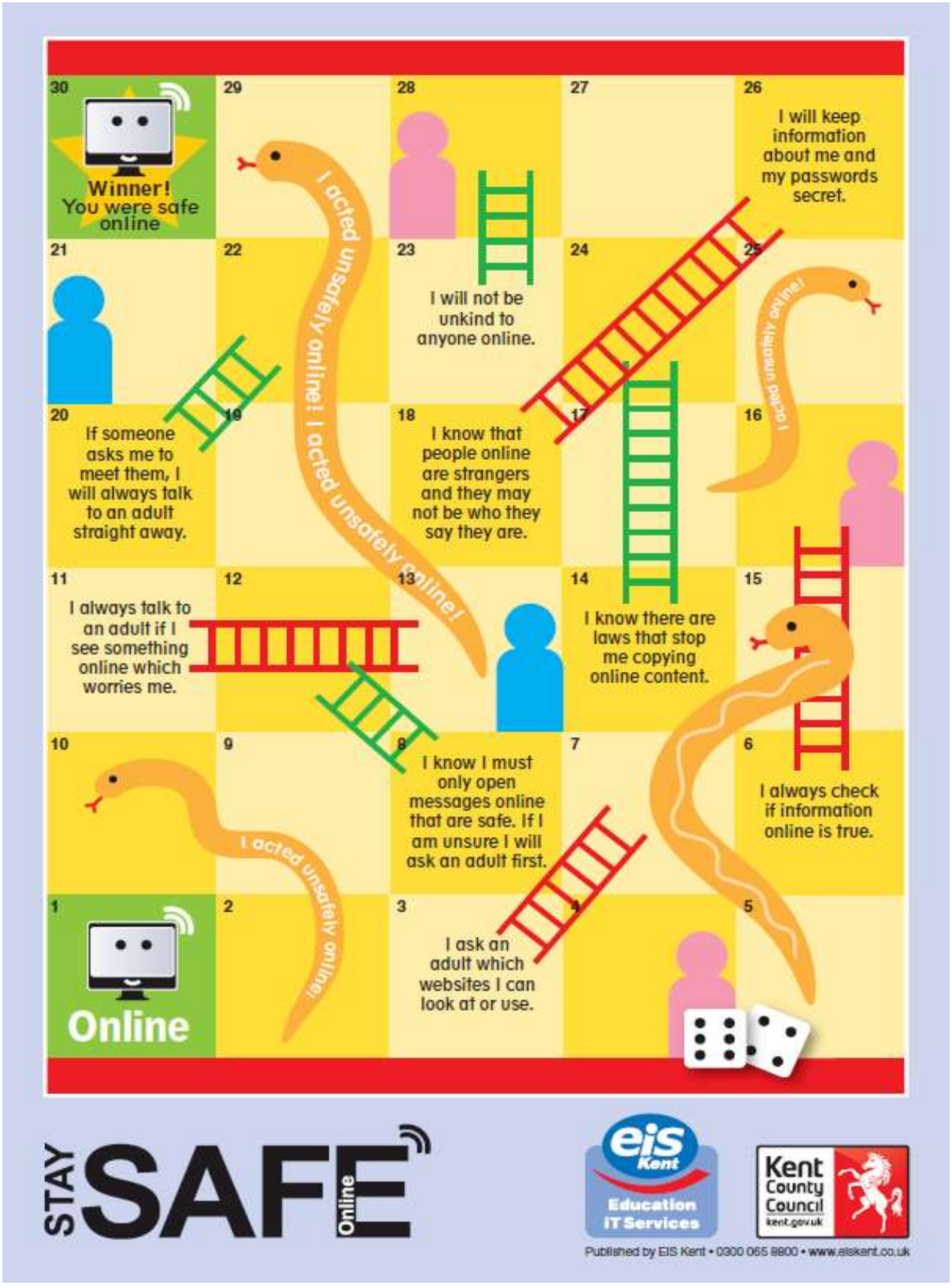
- I know that I will be able to use the internet in school, for a variety of reasons, if I use it responsibly. However, I understand that if I do not, I may not be allowed to use the internet at school.
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these I should report it to a teacher or adult in school or a parent or carer at home.
- I will treat my password like my toothbrush! This means I will not share it with anyone (even my best friend), and I will log off when I have finished using the computer or device.
- I will protect myself by never telling anyone I meet online my address, my telephone number, my school's name or by sending a picture of myself without permission from a teacher or other adult.
- I will never arrange to meet anyone I have met online alone in person without talking to a trusted adult.
- If I get unpleasant, rude or bullying emails or messages, I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- I will always be myself and not pretend to be anyone or anything I am not. I know that posting anonymous messages or pretending to be someone else is not allowed.
- I will always check before I download software or data from the internet. I know that information on the internet may not be reliable and it sometimes needs checking.
- If I bring in memory sticks / CDs from outside of school I will always give them to my teacher, so they can be checked for viruses and content, before opening them.
- I will be polite and sensible when I message people online and I know that sending a message is the same as having a conversation with someone. I will not be rude or hurt someone's feelings online.

- I know that I am not allowed on personal email, social networking sites or instant messaging in school.
- If, for any reason, I need to bring my mobile phone into school I know that it is to be handed in to the office and then collected at the end of the school day.
- I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.

Shortened version (for use on posters)

- I ask a teacher about which websites I can use
- I will not assume information online is true
- I know there are laws that stop me copying online content
- I know I must only open online messages that are safe. If I'm unsure I won't open it without speaking to an adult first
- I know that people online are strangers and they may not always be who they say they are
- If someone online suggests meeting up, I will always talk to an adult straight away
- I will not use technology to be unkind to people
- I will keep information about me and my passwords private
- I always talk to an adult if I see something which makes me feel worried

KS2 Acceptable Use Poster



Key Stage 3/4/5 (11-18)

Some statements are duplicated - settings will need to consider the best approaches for their students.

Possible Statements

- Schools should include specific information and expectations relating to use of devices in school for example, tablets, cloud computing, pupil owned devices.
- I know that school computers and internet access has been provided to help me with my learning and that other use of technology may not be allowed. If I'm not sure if something is allowed, I will ask a member of staff
- I know that my use of school computers/devices and internet access will be monitored
- I will keep my password safe and private as my privacy, school work and safety must be protected
- I will write emails and online messages carefully and politely; as I know they could be forwarded or seen by someone I did not intend
- I will only use social media sites with permission and at the times that are allowed. (Amend according to social media policy)
- I know that people I meet online may not be who they say they are. If someone online suggests meeting up then I will immediately talk to an adult and will always arrange to meet in a public place, with a trusted adult present
- I know that bullying in any form (on and off line) is not tolerated and I know that technology should not be used for harassment
- I *will* not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community
- I understand that it may be a criminal offence or breach of the school policy to download or share inappropriate pictures, videos or other material online. I also understand that it is against the law to take, save or send indecent images of anyone under the age of 18 and will visit www.thinkuknow.co.uk
- I will protect my personal information online
- I will not access or change other people files, accounts or information
- I will only upload appropriate pictures or videos of others online and when I have permission
- I will only use my personal device/mobile phone in school if I have permission from a teacher (Other specific statements will be required if mobile phones/personal devices are or are not permitted)
- I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources
- I will always check that any information I use online is reliable and accurate
- I will make sure that my internet use is safe and legal, and I am aware that online actions have offline consequences

- I will only change the settings on the computer if a teacher/technician has allowed me to
- I know that use of the schools' ICT system for personal financial gain, gambling, political purposes or advertising is not allowed
- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- I know that if the school suspect that I am behaving inappropriately with technology, then enhanced monitoring and procedures may be used, such as checking and/or confiscating personal technologies such as mobile phones and other devices
- I know that if I do not follow the AUP then:
    - List school sanctions
- If I am aware of anyone trying to misuse technology, I will report it to a member of staff
- I will speak to an adult I trust if something happens to either myself or another student which makes me feel worried, scared or uncomfortable
- I will visit www.thinkuknow.co.uk www.childnet.com and www.childline.org.uk to find out more about keeping safe online
- I have read and talked about these rules with my parents/carers

Alternatives

These headers are suggestions only; we encourage educational settings to work with learners to amend them accordingly.

Safe

- I will make sure that my internet use is safe and legal, and I am aware that online actions have offline consequences
- I know that my use of school computers, devices and internet access will be monitored to protect me and ensure I comply with the schools' acceptable use policy
- I know that people online aren't always who they say they are and that I must always talk to an adult before meeting any online contacts

Private

- I will keep my passwords private
- I know I must always check my privacy settings are safe and private
- I will think before a share personal information and/or seek advice from an adult
- I will keep my password safe and private as my privacy, school work and safety must be protected

Responsible

- Schools should include specific information and expectations relating to use of devices in school for example, tablets, cloud computing, pupil owned devices.
- I will not access or change other people files, accounts or information

- I will only upload appropriate pictures or videos of others online and when I have permission
- I will only use my personal device/mobile phone in school if I have permission from a teacher (Other specific statements will be required if mobile phones/personal devices are or are not permitted)
- I know I must respect the schools' systems and equipment and if I cannot be responsible then I will lose the right to use them
- I know that school computers, devices and internet access has been provided to help me with my learning and that other use of technology may not be allowed. If I'm not sure if something is allowed, I will ask a member of staff
- I will write emails and online messages carefully and politely; as I know they could be forwarded or seen by someone I did not intend
- I will only change the settings on the computer if a teacher/technician has allowed me to
- I know that use of the schools' ICT system for personal financial gain, gambling, political purposes or advertising is not allowed
- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- I know that if the school suspect that I am behaving inappropriately with technology, then enhanced monitoring and procedures may be used, such as checking and/or confiscating personal technologies such as mobile phones and other devices
- I know that if I do not follow the AUP then:
    - List school sanctions

Kind

- I know that bullying in any form (on and off line) is not tolerated and I know that technology should not be used for harassment
- I will not upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community I will always think before I post as once I upload text, photos or videos they can become public and impossible to delete
- I will not use technology to be unkind to people

Legal

- I know it can be a criminal offence to hack accounts or systems or send threatening and offensive messages
- I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources
- I understand that it may be a criminal offence or breach of the school policy to download or share inappropriate pictures, videos or other material online.

Reliable

- I will always check that any information I use online is reliable and accurate
- I know that people I meet online may not be who they say they are. If someone online suggests meeting up then I will immediately talk to an adult and will always arrange to meet in a public place, with a trusted adult present

Report

- If I am aware of anyone trying to misuse technology, I will report it to a member of staff
- I will speak to an adult I trust if something happens to either myself or another student which makes me feel worried, scared or uncomfortable
- I will visit www.thinkuknow.co.uk www.childnet.com and www.childline.org.uk to find out more about keeping safe online
- I have read and talked about these rules with my parents/carers

Shortened version (for use on posters)

Responsible

- I know I must respect the schools' systems and equipment and if I cannot be responsible then I will lose the right to use them
- I know that online content might not always be true
- I know my online actions have offline consequences
- I will always think before I post as once I upload text, photos or videos they can become public and impossible to delete
- I will not use technology to be unkind to people

Private

- I will keep my password and personal information private
- I know I must always check my privacy settings are safe and private

Legal

- I know that my internet use is monitored to protect me and ensure I comply with the schools' acceptable use policy
- I am aware that copyright laws exist, and I need to ask permission before using other people's content and acknowledge any sources I use
- I know it can be a criminal offence to hack accounts or systems or send threatening and offensive messages

Report

- I know that people online aren't always who they say they are and that I must always talk to an adult before meeting any online contacts
- If anything happens online which makes me feel worried or uncomfortable then I will speak to an adult I trust and visit www.thinkuknow.co.uk

AUP brief statement

This statement ***may be helpful to include on a setting website, or as part of transition documents to welcome new learners.***

At <**school name**> we want to ensure that all members of our community are safe and responsible users of technology. We will support our learners to…

- Become empowered and responsible digital creators and users
- Use our resources and technology safely, carefully and responsibly
- Be kind online and help us to create a community that is respectful and caring, on and offline
- Be safe and sensible online and always know that you can talk to a trusted adult if you need help

KS3/4 Acceptable Use Poster

Learners with SEND: based on ability levels

Learners functioning at Levels P4 –P7

- I ask a grown up if I want to use the computer
- I make good choices on the computer
- I use kind words on the internet
- If I see something I don't like online I tell a grown up
- I know that if I do not follow the school rules then:
    - List school sanctions

Learners functioning at Levels P7-L1 (Based on Childnet's SMART Rules: www.childnet.com)

Safe

- I ask a grown up if I want to use the computer
- On the internet I don't tell strangers my name
- I know that if I do not follow the school rules then:
    - List school sanctions

Meeting

- I tell a grown up if I want to talk on the internet

Accepting

- I don't open emails from strangers

Reliable

- I make good choices on the computer

Tell

- I use kind words on the internet
- If I see something I don't like online I will tell a grown up

Learners functioning at Levels L2-4 (Based on SMART Rules: www.childnet.com)

Safe

- I ask an adult if I want to use the internet
- I keep my information private on the internet
- I am careful if I share photos online
- I know that if I do not follow the school rules then:
    - List school sanctions

Meeting

- I tell an adult if I want to talk to people on the internet
- If I meet someone online I talk to an adult

Accepting

- I don’t open messages from strangers
- I check web links to make sure they are safe

Reliable

- I make good choices on the internet
- I check the information I see online

Tell

- I use kind words on the internet
- If someone is mean online then I don’t reply, I save the message and show an adult
- If I see something online I don’t like, I will tell a teacher

Sample Letter for Learners

Dear child's name

All pupils at our school use computer facilities, including internet access, as an essential part of learning in today's modern British Society. You will have the opportunity to access a wide range of technology resources. This includes access to: [adapt for individual school, this list is not exhaustive]

- Computers, laptops and other digital devices
- The Internet, which may include search engines and educational sites
- School learning platform/intranet
- Email
- Games consoles and other games-based technologies
- Digital cameras, webcams and video cameras

At < school name> we recognise the essential and important contribution that technology plays in promoting your learning and development, both at school and at home. However, we also recognise there are potential risks. The school will take all reasonable precautions to ensure that you are as safe as possible when using school equipment and will work together with you and your family to help you stay safe online. (School may wish to include specific details for example, filtering, monitoring and expectations regarding use of personal devices)

At <school name> we want to ensure that all members of our community are safe and responsible uses of technology. We will support you to:

- Become empowered and responsible digital creators and users
- Use our resources and technology safely, carefully and responsibly
- Be kind online and help us to create a community that is respectful and caring, on and offline
- Be safe and sensible online, and always know that you can talk to a trusted adult if you need help

Should you have any worries about online safety then you can speak with (name of tutor and or named member of staff). You can also access support through the school (list pastoral support contacts) and via other websites such as www.thinkuknow.co.uk and www.childline.org.uk (List other websites or support services as appropriate)

We request that you and your family read our school Acceptable Use Policy and return the attached slip. We look forward to helping you become a positive and responsible digital citizen.

Yours sincerely,
Headteacher

Learner Acceptable Use Policy Agreement Form

It is recommended settings attach a copy of the AUP to this form.

<School Name> Acceptable Use Policy - Pupil Response

I, with my parents/carers, have read and understood the pupil Acceptable Use Policy (AUP).

I agree to follow the pupil AUP when:

1. I use school systems and devices, both on and offsite
2. I use my own devices in school, when allowed, including mobile phones, gaming devices, and cameras. (amend or remove in accordance with settings online safety/personal devices policy)
3. I use my own equipment out of the school, in a way that is related to me being a member of the school community, including communicating with other members of the school, accessing school email, learning platform or website. (amend as appropriate)

Name…… Signed…….

Class…… Date…….

Parents Name…….....

Parents Signature…….

Date…….

Sample Letter for Parents and Carers

Dear Parent/Carer

All pupils at <**school name**> use computer facilities and internet access, as an essential part of learning as required by the National Curriculum. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes access to: [adapt for individual school, this list is not exhaustive]

- Computers, laptops and other digital devices
- The Internet, which may include search engines and educational sites
- School learning platform/intranet
- Email
- Games consoles and other games-based technologies
- Digital cameras, webcams and video cameras

< **school name**> recognises the essential and important contribution that technology plays in promoting children's learning and development, believe it and offers a fantastic range of positive activities and experiences. We do recognise however that this can bring risks. We take your child's online safety seriously and, as such, will take all reasonable precautions, including monitoring and filtering systems, to ensure that pupils are safe when they use our internet and systems. This includes: School should include specific details about precautions taken, such as use of devices, appropriate supervision, education and curriculum approaches. The school must then ensure that these precautions are in place.

We recognise however that no technical system can replace online safety education and believe that children themselves have an important role to play in developing responsible behaviour. To support the school in developing your child's knowledge and understanding about online safety, we request that you read the attached Acceptable Use Policy with your child, discuss the content with them and return the attached slip.

(Additional Paragraph for Early Years/KS1/SEND**)** *We understand that your child is too young to give informed consent on his/ her own; however, we feel it is good practice to involve them as much as possible in the decision-making process, and believe a shared commitment is the most successful way to achieve this.*

Hopefully, you will also find this Acceptable Use Policy provides you with an opportunity for conversations between you and your child about safe and appropriate use of the technology, both at school and at home.

We request that all parents support our approach to online safety by role modelling safe and positive online behaviour and by discussing online safety whenever children access technology at home. Parents can visit the school website's (link) for more information about our approach to online safety. Full details of the school's online safety policy are available on

the school website (**insert link**) or on request. Parents/carers may also like to visit the following links for more information about keeping children safe online:

- www.thinkuknow.co.uk
- www.childnet.com
- www.nspcc.org.uk/onlinesafety
- www.saferinternet.org.uk
- www.internetmatters.org

Should you wish to discuss the matter further, please do not hesitate to contact the Designated Safeguarding Lead (**name**) or myself.

Yours sincerely,

Headteacher

Parent/Carer Acknowledgement Form

Pupil Acceptable Use Policy: <school name> School Parental Acknowledgment

I, with my child, have read and discussed <**school name** > Pupil Acceptable Use Policy.

I am aware that any internet and computer use using school equipment may be monitored for safety and security reason to safeguard both my child and the schools' systems. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy or have any concerns about my child's safety.

I will inform the school or other relevant organisations if I have concerns over my child's or other members of the school communities' safety online.

I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I will support the schools online safety approaches and will encourage my child to adopt safe use of the internet and digital technologies at home.

Child's Name…….

Signed (**if appropriate**) …….

Class…… Date…….

Parents Name…….....

Parents Signature……. Date…….

Sample Parent/Carers Acceptable Use Policy

Note: Please be aware that if parents/carers refuse to sign and agree the AUP, this can cause issues for learning as children will need to use the internet to access the curriculum. Setting should have a robust process in place to manage and record parental responses and to engage with parents who do not respond. Alternatives include highlighting online safety within the Home School Agreement or using an acknowledgement form for the AUP.

1. I have read and discussed <**school name** > Acceptable Use Policy with my child.
2. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.
3. I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons, to safeguard both my child and the schools' systems. This monitoring will take place in accordance with data protection (including GDPR) and human rights legislation.
4. I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
5. I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted.
6. I understand that if my child does not abide by the school Acceptable Use Policy then sanctions will be applied in line with the school policies including behaviour, online safety and anti-bullying policy (**as appropriate**). If the school believes that my child has committed a criminal offence then the Police will be contacted.
7. I, together with my child, will support the school's approach to online safety and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.
8. I know that I can speak to the school Designated Safeguarding Lead (**Name**), my child's teacher or the headteacher if I have any concerns about online safety.
9. I will visit the school website (**link**) for more information about the school's approach to online safety as well as to access useful links to support both myself and my child in keeping safe online at home.
10. I will visit the following websites for more information about keeping my child(ren) safe online:
    - www.thinkuknow.co.uk/parents,
    - www.nspcc.org.uk/onlinesafety

- www.internetmatters.org
- www.saferinternet.org.uk
- www.childnet.com

11. I will support the school and my child by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing online safety with them when they access technology at home.

I have read, understood and agree to comply with the <school name >Acceptable Use Policy.

Child's Name…… Class……

Parents Name…….....

Parents Signature……

Date…….

Staff Acceptable Use Policy 2018

For staff (including visitors/volunteers) who access school ICT systems

As a professional organisation with responsibility for safeguarding, it is important that 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 technology, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list; all members of staff 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. (**Include school information and requirements for example, how often they should be changed**)

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 or CDs) will be suitably protected. This may include data being encrypted by a method approved by the school. **(Amend and include specific details as appropriate).**
- Any images or videos of pupils will only be used as stated in the school image use policy (**link**) 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 the School Learning Platform to upload any work documents and files in a password protected environment or via VPN. (**Amend as appropriate**)

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'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. **Note: Schools should ensure the online safety policy includes specific details and expectations regarding safe practice relating to the specific use of technology within school.**

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

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 ICT Support Provider/Team/lead (**named contact**) as 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.

- Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead (**name**) and/or headteacher.

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 as outlined in the **Online Safety/Social Media policy** (**link**) 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 code of conduct/behaviour policy** 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 (**name**) **and/or** the headteacher.

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.

I have read, understood and agreed to comply with <school name > Staff Acceptable Use Policy

Name: …… Signed: …….... Date: ……

Sample Letter for Staff

Please note this letter does NOT replace the Staff AUP

Dear member of staff name

At <school name> we recognise that staff can be vulnerable to online risks. Social media can blur the definitions of personal and working lives; it is important that all members of staff at <school name> take precautions to protect themselves both professionally and personally online. We request that all members of staff:

- Are conscious of their own professional reputation and that of the school when 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.
  - Content shared online cannot be guaranteed to be "private" and could potentially be seen by unintended audiences. This could have consequences including civil, legal and disciplinary action being taken.

- Are aware that as professionals, we must ensure that the content we post online does not bring the school or our professional role into disrepute and does not undermine professional confidence in our abilities.
  - The teaching standards state that as professionals we should be achieving the highest possible standards in our conduct, act with honesty and integrity and forge positive professional relationships.

- All Staff be careful when publishing any information, personal contact details, video or images online.
  - 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.
  - Ensure that the privacy settings of the social media sites you use are set appropriately.
  - Consider if you would feel comfortable about a current or prospective employer, colleague, child in your care or their parent/carer, viewing or sharing your content. If the answer is no, consider if it should be posted online at all.

- Do not 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.

- If you have a pre-existing relationship with a child or parent/carer or any other situation that may compromise this, speak to the Designated Safeguarding Lead (name).

- Always use a work provided email address or phone number to contact children and parents – this is essential to protect yourself as well as the wider community.

- If you are concerned about a child's wellbeing or online behaviour, please speak to the Designated Safeguarding Lead (name). If you are targeted online by a member of the community or are concerned about a colleague, then please speak to the headteacher and/or chair of governors (name).
    - If you are unhappy with the response you receive, or do not feel able to speak to the Designated Safeguarding Lead, headteacher or chair of governors then we request you follow our Whistleblowing procedure (link)

- If you have any questions regarding online conduct expected of staff, please speak to the Designated Safeguarding Lead (name) and/or headteacher.

Documents called "Cyberbullying: Supporting School Staff", "Cyberbullying: advice for headteachers and school staff" and "Safer professional practise with technology" are available in the staffroom (or other locations for example school intranet) to help you consider how to protect yourself online.

Please photocopy them if you want or download the documents directly from:

- www.childnet.com/teachers-and-professionals/for-you-as-a-professional
- www.gov.uk/government/publications/preventing-and-tackling-bullying
- www.saferinternet.org.uk
- www.kscb.org.uk/guidance/online-safety

Additional advice and guidance for professionals is available locally through the Education Safeguarding Service or nationally through Professional Unions and/or the Professional Online Safety helpline www.saferinternet.org.uk/about/helpline

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 behaviour policy/code of conduct could lead to disciplinary action; it is crucial that all staff understand how to protect themselves online.

Please speak to your line manager, the Designated Safeguarding Lead (name) or myself if you have any queries or concerns regarding this.

Yours sincerely,

Headteacher

Additional regarding online participation on behalf the School, if applicable

The principles and guidelines below set out the standards of behaviour expected of you as an employee of the school. If you are participating in online activity as part of your capacity as an employee of the school, we request that you:

- Be professional and remember that you are an ambassador for the school. Disclose your position but always make it clear that you do not necessarily speak on behalf of the school.
- Be responsible and honest and consider how the information you are publishing could be perceived
- Be credible, accurate, fair and thorough.
- Always act within the legal frameworks you would adhere to within school, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Be accountable and do not disclose information, make commitments or engage in activities on behalf of the school unless you are authorised to do so.
- Always inform your line manager, the designated safeguarding lead and/or the headteacher of any concerns such as criticism or inappropriate content posted online.

Visitor/Volunteer Acceptable Use Policy

For visitors/volunteers and staff who do not access school ICT systems

As a professional organisation with responsibility for children's safeguarding it is important that all members of the community, including visitors and volunteers, are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy.

This is not an exhaustive list; visitors/volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I will ensure that any personal data of learners, staff or parents/carers is kept in accordance with Data Protection legislation, including GDPR. Any data which is being removed from the site, such as via email or on memory sticks or CDs, will be encrypted by a method approved by the setting. Any images or videos of learners will only be used as stated in the school image use policy and will always reflect parental consent. (**This statement is only required if visitors/volunteers have access to data**)

2. 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.

3. I will follow the school's policy regarding confidentially, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

4. 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.
    - All communication will take place via school approved communication channels such as via a school provided email address or telephone number and not via personal devices or communication channels such as via personal email, social networking or mobile phones.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead (name) and/or headteacher.

5. My use of ICT and information systems will be compatible with my role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. I will take appropriate steps to protect myself online and my use of ICT will not interfere with my work duties and will always be in accordance with the school AUP and the Law.

6. 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.

7. I will promote online safety with the children 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.

8. 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 (name) or the headteacher.

9. I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead (name) as soon as possible.

10. I understand that if the school believes inappropriate use or unacceptable behaviour is taking place, the school may invoke its disciplinary procedure. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with the <school name >Visitor /Volunteer Acceptable Use Policy.

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

Wi-Fi Acceptable Use Policy

For those using setting provided Wi-Fi. Settings may wish to use a paper or electronic AUP for guest access of Wi-Fi by members of the community. This template is provided for settings to adapt and use as appropriate.

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.

1. The school provides Wi-Fi for the school community and allows access for (**state purpose, for example education use only**). **Schools should include any include information about time limits, passwords and security.**

2. I am 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.

3. The use of ICT devices falls under <**school name**> school's Acceptable Use Policy, online safety policy and behaviour policy (any other relevant policies such as data security, safeguarding/child protection) which all pupils/staff/visitors and volunteers must agree to and comply with.

4. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

5. School owned information systems, including Wi-Fi, must be used lawfully; 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.

6. 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.

7. The school's wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.
8. The school accepts no responsibility for any software downloaded and/or installed, email 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.
9. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.
10. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.
11. I will not attempt to bypass any of the schools' security and filtering systems or download any unauthorised software or applications.
12. My use of 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.
13. 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.
14. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (name) as soon as possible.
15. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead (name) or the headteacher.
16. I understand that my use of the school Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with <school name > Wi-Fi Acceptable Use Policy.

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

PTA/Committee Social Networking Acceptable Use Policy

For parents/volunteers running official social media accounts, for example PTA groups and committees

1. As part of the school's drive to encourage safe and appropriate behaviour online, I will support the school's approach to online safety. I am aware that (name tool using, e.g. Facebook, Twitter) is a public and global communication tool and any content posted may reflect on the school, its reputation and services.

2. I will not use the site/page/group 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.

3. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Designated Safeguarding Lead (name) or the headteacher.
    - The headteacher (or other appropriate member of leadership) retains the right to remove or approve content posted on behalf of the school.
    - Where it believes unauthorised and/or inappropriate use of the (tool using) 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.

4. 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.

5. I will follow the school's policy regarding confidentiality and data protection/use of images.
    - 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 via school owned devices. Images taken for the sole purpose of inclusion on (tool using) will not be forwarded to any other person or organisation.

6. I will promote online safety in the use of (tool using) and will help to develop a responsible attitude to safety online and to the content that is accessed or created.

7. I will set up a specific account/profile using a school provided email address to administrate the site and I will use a strong password to secure the account.
    - The school Designated Safeguarding Lead (name) and/or school management team (amend as appropriate) will have full admin rights to the account.

8. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used. I 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 Designated Safeguarding Lead (name) and/or headteacher immediately.

10. I will ensure that the (tool using) is moderated on a regular basis as agreed with the Designated Safeguarding Lead (name) and/or headteacher.

11. I have read and understood the school online 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 headteacher.

12. If I have any queries or questions regarding safe and acceptable practise online, I will raise them with the Designated Safeguarding Lead (name) or the headteacher.

I have read, understood and agree to comply with <school name > PTA/committee Social Networking Acceptable Use Policy

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

Accepted by: ……. Print Name: …….

Official Social Networking Acceptable Use Policy for Staff

For use with staff running official school social media accounts

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. I am aware that the (tool using e.g. Facebook, Twitter) is a public and global communication tool and that any content posted may reflect on the school, its reputation and services.

2. I will not use the site/page/group 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.

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

4. 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.

5. I will follow the school's policy regarding confidentiality and data protection/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 via school owned devices. Images taken for the sole purpose of inclusion on (tool using) will not be forwarded to any other person or organisation.

6. I will promote online safety in the use of (tool using) 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 the Designated Safeguarding Lead/headteacher prior to use.

7. I will set up a specific account/profile using a school provided email address to administrate the account/site/page (tool using) and I will use a strong password to secure the account. Personal social networking accounts or email addresses will not be used.

- The school Designated Safeguarding Lead and/or headteacher will have full admin rights to the (tool using) site/page/group.

8. Where it believes unauthorised and/or inappropriate use of the (tool using) 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.

9. 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.

10. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the headteacher and/or Designated Safeguarding Lead urgently.

11. I will ensure that the (tool using) site/page is moderated on a regular basis as agreed with the school Designated Safeguarding Lead.

12. I have read and understood the school online safety policy which covers the requirements for safe IT use, including using appropriate devices and the use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the headteacher.

13. If I have any queries or questions regarding safe and acceptable practise online I will raise them with the Designated Safeguarding Lead (name) or the headteacher.

I have read, understood and agree to comply with the <school name > Social Networking Acceptable Use policy.

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

Accepted by: ……. Print Name: …….

Acknowledgements and thanks

This document and statements have been produced with thanks to members of Kent Online Safety Strategy Group and material from UK Safer Internet Centre, South West Grid for Learning, Childnet and CEOP.

Additional thanks to The Judd School, Kingsnorth Primary School, Loose Primary School, Peter Banbury, Kent Police, Kent Schools Personnel Service (SPS), Kent Legal Services and Kent Libraries and Archives, for providing comments, feedback and support on previous versions.

Disclaimer

The Education People make every effort to ensure that the information in this document is accurate and up-to-date. If errors are brought to our attention, we will correct them as soon as practicable.