Acceptable Use Policies for Education Settings and their Wider Communities

Considerations and Templates for Acceptable Use Policies (AUPs) for Children, Young People, Parents/Carers, Staff, Volunteers, Visitors and other Community Members

3rd Edition, August 2016

Kent County Council Online safety (e-Safety) Strategy Group

Contents

Acceptable Use Policies for Education Settings and their Wider Communities

Guidance for use

This document was written by the Kent Online Safety (e-Safety) strategy group and approved by the Kent Safeguarding Children's Board Education Subgroup.

This AUP template is suitable for all educational settings including (but not limited to) schools, early year's settings, Pupil Referral Units, 14-19 settings, alternative curriculum provisions, Children Centre's, Childminders and hospital schools etc. We encourage all education establishments to ensure that their AUP is fit for purpose and individualised for their context. 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.

This template has been produced by children and young people, schools, child protection officers, multi-agency children's workforce professionals and Kent Police to help schools and other educational settings write Acceptable Use Policies (AUP).

Aims of the guidance and template

The following information is provided as a template for educational settings and for leadership staff to use to update their policies and content. This document may be used as part of an action plan or calendar of events to enable schools to embed Online safety (Online safety (e-Safety) practice. Not all templates within this document will be required and settings are encouraged to ensure that their AUPs reflect their own needs and requirements and settings are urged to use these documents as a basis to start from and to develop the AUP specifically for their own technologies and communities.

Schools and settings should work in partnership with their own communities (e.g. staff, pupil councils, parent groups etc) to ensure that the AUP documents are adapted specifically to reflect the needs and requirements of the school and ensure that all members of the community have clear understanding, awareness and 'ownership' of the policy.

Structure of the guidance and template

Elements in the AUP template highlighted in red are areas where schools may wish to personalise the template by referencing their own specific policies and procedures such as staff behaviour/codes of conduct, data security, image use, online safety (e-Safety), pupil behaviour, anti-bullying and safeguarding and child protection. Schools may also consider providing a written process or chart to follow for reporting any incidents or concerns to ensure that all members of staff are aware of and understand the school's specific safeguarding procedures.

This document suggests a range of statements and should be used to develop the settings online safety (e-Safety) ethos and whole-community approach.

Keeping policies up-to-date

It is strongly recommended that education settings revise their Acceptable Use Policies (AUP) at least annually to reflect changes and advancements in technology. They must also be revised following any local or national guidance or legislation changes.

Schools and settings should also revisit their AUPs following any online safety concerns within their community to implement any lessons learnt or highlight any good practice. Schools and settings should also review and update AUPs when introducing new technology and systems to ensure there are clear expectations regarding safe and responsible use.

Due to the constantly evolving nature of technology (including local and national guidance and legislation) this document will be updated frequently. Leaders and managers are encouraged to make a

note of the edition version used and check Kelsi for updates. Alternatively leaders should subscribe to the Kent e-Safety blog for email alerts https://kentesafety.wordpress.com/

Questions and queries

If Kent education settings wish to discuss this document or any other online safety concerns, please contact the Kent County Council Education Safeguarding Adviser (Online Protection) or e-Safety Development Officer via esafetyofficer@kent.gov.uk

What is an Acceptable Use Policy?

Leadership Teams and managers within education settings will be encouraging and supporting 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 is carefully managed by educational settings to ensure that all members of the community (including their data) are kept safe and that online risks and dangers are recognised by the setting and mitigated. Acceptable Use Policies (AUP) should be an integral and essential part of this process.

An AUP:

- Is a clear and concise document which gives all users an outline of acceptable and unacceptable behaviours
- Should be developed with end-user (e.g. children, staff) input to engage and empower all members of the school community
- Is appropriate to the school needs and requirements. Schools will need different versions for different audiences within the community
- Is embedded as part of induction and new intake
- Is developed by the online safety (e-Safety) Coordinator as part of senior 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 the school site or those provided by the school
- 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 school for support or questions
- Must be monitored, reviewed and updated regularly by senior leaders/managers

AUPs should be reviewed regularly (at least annually) to check they are appropriate to the settings needs and requirements. AUPs should be revisited and updated by settings 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 must be communicated and shared with all members of the community.

Where the school/setting outsources any ICT services or other systems and services, it is essential that an AUP is created as part of the service level agreement and is owned and enforced by both the managed service provider and the school/setting.

The AUP is a crucial tool for managers and senior leaders in education settings to identify and establish online safety as part of the whole school safeguarding culture. It should focus on the behaviours rather than the technology itself and will need to be adapted according to settings own approaches and ethos. The AUP should also be developed with the involvement of members of the school community to ensure that it reflects the ethos and nature of the school. The AUP should be embedded as part of the wider education and curriculum provision and be appropriate to pupils needs, taking account age and ability and should be viewed as an essential part of school induction and training.

Acceptable Use Policies for staff, visitors and volunteers

Why do we need an AUP for staff, visitors and volunteers?

Leadership Teams (LT) and managers will be encouraging and supporting the positive use of Information and Communication Technology (ICT) to develop both formal and informal learning opportunities in schools and settings. It is essential that the use of ICT and online tools is carefully managed to ensure that all members of the school community are kept safe as well as their data and that risks or dangers are recognised and mitigated. The staff AUP should therefore be developed by a member leadership/management and must be approved by the Head Teacher/Manager, designated Safeguarding Lead (DSL) and Governing Body/Trust as appropriate. The AUP must also link in with or be embedded within existing school/setting policies such as staff codes of conducts or staff handbooks which must outline the settings expectations regarding appropriate and professional behaviours.

Leaders, governing bodies and proprietors should be aware of the statutory duties and responsibilities placed upon schools and colleges within "Keeping Children Safe in Education" 2016.This guidance can be found at https://www.gov.uk/government/publications/keeping-children-safe-in-education--2 '

Keeping children safe in Education' 2016 (published on the 26th May 2016 to be implemented in September) 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:

- *an effective child protection policy; and*
- *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. (p.14-15)*

It is therefore essential that leaders, governing bodies and proprietors ensure that their setting have an appropriate AUP in place which covers the requirements as identified within keeping children safe in education 2016.

It is important that schools and settings also acknowledge national and local guidance when developing their AUP. Some key guidance which will affect schools includes the Teaching Standards DfE: https://www.gov.uk/government/collections/teachers-standards.

The preamble of the Teaching standards 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*."

School and settings leaders and managers should also access "Guidance for Safer Working Practice for Adults who Work with Children and Young People" (2015), which contains useful guidance around professional use of technology. http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/safeguarding-policies-and-guidance

Schools and settings may wish to read relevant legislation and information regarding this document and amend the school's AUP accordingly. Schools and settings have a duty of care to safeguard and protect staff under the Health and Safety at Work Act 1974 and the Management of Health and Safety at Work Regulations 1999. Key legislation also includes Section 11 of the Children Act 2004 which 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.

Schools must also ensure they comply with the Data Protection Act (DPA) 1998. Under the DPA every organisation that processes personal information (personal data) must notify (register with) the Information Commissioner's Office, unless they are exempt.

Specific guidance for education establishments, including information on how to register and check notification may be found on the ICO website:
www.ico.gov.uk/for_organisations/sector_guides/education.aspx.

The DPA applies to anyone who handles or has access to information concerning individuals and everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. Schools should have a Data Protection and Security Policy in place to outline the legal responsibilities and actions taken to protect personal data in accordance with the DPA. This may include password safety, not sharing login information, use of encryption, use of encrypted and/or school provided laptops/devices, secure email and encrypted portable data storage devices (e.g. memory sticks) etc. KCC Data Protection information may be seen at: www.kelsi.org.uk and schools can read more information from the Information Commissioner's Office: http://www.ico.gov.uk/

An 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 school and all members of staff comply with the appropriate legal responsibilities, the reputation of the school is maintained and the safety of all users is ensured. Members of staff are entitled to seek their own legal advice on this matter before signing the AUP.

How should schools/settings develop and implement an AUP for staff, visitors and volunteers?

It is strongly recommended that members of staff should be actively involved in creating the school AUP. This may include using inviting staff to contribute and express views and opinions. This will enable schools to ensure that the AUP is appropriate and reflects the needs and requirements of the establishment. All members of staff (including visitors and volunteers) should read, understand and sign the AUP before being granted access to any of the schools' ICT systems It is therefore essential that the AUP is firmly embedded within the school induction process for all members of staff (including any volunteers, part-time staff or work experience placements).

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 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. It is also important that all members of staff receive up-to-date and relevant training around this issue on a regular basis to ensure that the AUP is understood and supported throughout the staff group.

All adults who work within the school either as employees or volunteers (including all teaching, non-teaching staff, volunteers, PTA groups, Governors etc.) must be aware of the school 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. The AUP should form an essential part of the schools induction process for both formal recruitment and for others staff who may have access staff, children, school information, ICT systems or be considered to be representing the school including Governors, committee members, volunteers and visitors.

Considerations within an AUP for staff

It is essential that schools and settings put in place clear professional boundaries for all members of staff, regardless of their role and status. This will apply to the whole staff group, including teaching and non-teaching staff, volunteers (including governors, parent helpers etc.) and external contractors.

Some schools may wish to provide more explicit guidance for staff, volunteers and visitors around use of social networking and email as, even when use of social media sites such as YouTube, Facebook and Twitter occur in their own time using their own computer or devices, it can leave staff vulnerable to abuse or a blurring of professional boundaries. Schools must be aware they cannot ban staff from using social networking sites in their own personal time; however they can and should provide advice for staff and put in place appropriate guidance and boundaries around interaction with pupils and parents/carers. It is recommended that any contact with pupils and parents (past or present) only takes place via school approved and provided communication channels, e.g. school email address or the school learning platform, so it can be monitored and traced in the case of an allegation or concern.

However, schools must recognise that in some cases there may be pre-existing or external relationships which mean that a total “ban” from adding pupils or parents, past or present, as friends or contacts on personal social networking sites may be difficult to enforce, such as where pupils or parents are family members of staff. Members of staff should be instructed to make their line manager and/or leadership team aware of these exceptions in order to protect themselves from allegations or misinterpreted situations. Leaders should make their expectations regarding online contact between staff and pupils explicitly clear as part of regular staff training and induction and all staff should ensure that any contact between staff and pupils and parents takes place within clear and explicit professional boundaries and be transparent and open to scrutiny at all times.

It is crucial that all members of staff are made aware of the boundaries and professional practices online in order to protect their professional status. Staff should be advised to regularly review their privacy settings on any personal social media sites they use, however they should always remember that once content is shared online it is possible for it be circulated more widely than intended without consent or knowledge (even if content is thought to have been deleted or privately shared). Many schools and settings are now choosing to use social media as a communication or teaching and learning tool and school AUPs must be updated to reflect this use in order to safeguard staff, pupils and the school. Specific AUPs to reflect the official use of social media by staff and volunteers are included within this document to support this.

Schools and settings may also wish to consider adding a statement regarding their policy on staff using school equipment for personal use. Occasional personal use of the school’s computers can be beneficial to the development of staff IT skills and to enable staff to maintain a positive work-life balance. However this is at the school’s discretion and can be revoked at any time. Staff should be made that it is their choice to use school systems for personal use and must be made aware that any use of school systems can and may be monitored. This is not in place to spy on members of staff’s personal life and must always be accordance of relevant privacy legislation. Leaders and managers should be aware that seizing and searching members of staffs’ personal devices or accounts may be unlawful. If leaders feel this is required or appropriate, for example if they believe a criminal offence may have been committed, then the appropriate agency should be informed.

Staff must appreciate that school systems must be safeguarded from misuse and any activity on school devices and systems could be checked if required. Any online behaviour and activity by a member of staff whilst using the school systems must be in accordance of the school AUP and any policies relating to staff conduct and personal use must not interfere with the member of staff’s duties or be for commercial purpose or gain (unless authorised by the leadership team/managers).

Considerations within an AUP for visitors and volunteers

It is important that schools and setting provide visitors and volunteers with clear expectations regarding professional behaviour. This is especially important to ensure school confidentiality policies are respected. For example a concern could arise if a parent volunteer posted comments on social media about another child's behaviour in the classroom then this could breach the schools confidentiality process.

Some visitors to schools and staff may have additional considerations which schools/settings may need to consider. For example, schools may wish to add additional statements or have a separate AUP for Governors or to support any members of staff that have a role in implementing and monitoring school ICT networks and infrastructure such as network managers and technicians.

In some situations, schools and settings may have visitors or volunteers who are not members of staff and yet they may need to have access to or use school systems or data, such as governors or visiting IT staff. It is therefore important that schools and settings work with visitors and volunteers to help ensure that the community is kept safe.

It's important that any visitors or volunteers are aware of any boundaries for use and therefore an AUP for visitors and volunteers is an important tool to safeguard the community. Examples have been provided within the document for schools to use and adapt. Schools and settings may wish to have a separate AUP for visitors and volunteers who use the schools/settings systems

Acceptable Use Policies for Children and Young People

Why do we need an AUP for children and young people?

An AUP should not be used to limit the ways in which children and young people use technology, but should aim to ensure that the children are protected and are educated about safe and appropriate online behaviour. Children and young people should be empowered and supported to take responsibility for their own use of new technologies and schools should work with families to enable children to use a range of technologies safely and responsibly. Schools have a duty of care to safeguard children and to take all reasonable steps to ensure that their internet use is lawful when at school. As highlighted within the 2015 Ofsted Common Inspection Framework and the "Inspecting Safeguarding" document, it is essential that schools and 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 in and out of school could have an impact both within and outside of school. Criminal, civil or disciplinary action could be taken, depending upon the child's age and the circumstances of the wrong committed. It is therefore important that the pupil AUP is supported with regular, embedded and progressive education for children, which clearly highlights safe and positive online behaviour that is appropriate to their age and ability.

This document provides a list of possible statements for AUPs for children and young people but will need to be adapted by the school according to their own online safety (e-Safety) ethos and approach as well as their individual requirements and systems. Whilst AUPs should be developed by a member of the leadership team and be approved by the Head Teacher/Manager and Governing Body as appropriate, it is strongly recommended that pupils should also be actively involved in creating the pupil AUP to ensure it is appropriate. This will also empower pupils and ensure that the online voice of the child is acknowledged by schools.

How should schools/settings develop and implement AUPs for children and young people?

In order to protect children, it is essential to have an AUP in place which has been viewed and discussed in a way which is appropriate to their age and abilities. All children who use ICT must be aware of the school expectations whether on or off site. The pupil AUP should be discussed with children on a regular basis as well as when they are actually using technology. This may feature within specific online safety (e-Safety) education but this must not be used in isolation, for example only mentioned within computing lessons. As pupils transition throughout the school, for example between key stages or ability levels, different versions of the AUP might be required for pupils due to the changes in how children use and access technology.

Schools will need to ensure that the AUP reflects pupil's use of school equipment and systems and will need to be adapted to state expectations regarding safe use. It is important for schools to ensure that the AUP for

pupils reflects the use of specific school systems such as tablets, cameras etc. It is especially important that the AUP reflects expectations for safe use of technology when schools are using any systems which are not fully under school control or when using external systems such as cloud storage, email, apps etc.

Schools may wish to consider adding a statement regarding children using school equipment for personal use. Occasional personal use of the school's computers can be beneficial to the development of IT skills, however this can bring safeguarding concerns and risks and should be at the school's discretion and can be revoked at any time. This approach should be carefully risk assessed by schools and appropriate safeguarding approaches such as filtering, monitoring and education must be in place. Schools may also want to consider adapting the AUP if they allow the use of personal devices (such as mobile phones) by pupils on-site according to their own policy and procedures. Any online behaviour and activity by a pupil should be in accordance with the school AUP and behaviour policy and not interfere with the pupil's education and comply with the law at all times.

All pupils must also be made aware that their internet and technology use may be recorded or monitored for safety and security reasons prior to internet or technology access. Schools will need to consider how pupil activity can be captured or monitored, such as through appropriate supervision or recording pupil logins to devices, systems or wireless internet access, when using tablets or devices, whether school owned or externally provided.

If schools use any additional monitoring products or systems to record the conduct of pupils when using school owned ICT systems, then they must ensure pupils are explicitly made aware of this activity prior to access. All monitoring must be in accordance with the law at all times.

The pupil AUP must be presented in a format which is accessible to all pupils, including those with special educational needs and disabilities. Schools may need to work with SENCOs and other specialist services to ensure that the AUP is accessible and understood by all pupils.

Pupils should be empowered to use technology safely and responsibly and the most productive approach to developing a pupil AUP is to involve and engage pupils directly in the process of creating and reviewing content. Schools may wish to undertake this by involving pupil/student councils or as part of wider whole school engagement e.g. as part of class or tutor discussions. To be successful, the pupil AUP needs to be included as part of an embedded and progressive online safety (e-Safety) curriculum. Children should be educated about safe and responsible use of technology prior to access and this will need to reinforce on a regular and consistent basis. Children need to be empowered and educated to maximise the potential of technology and also to enable them to minimise risks. The AUP statements need to be fully explored and discussed with children to ensure that they understand the statements, are aware of the consequences and know how to access support.

Engaging with parents/carers

The pupil AUP should be shared with parents/carers in order to develop a cohesive approach to online safety (e-Safety) as children and young people use technology as part of everyday family life. It's important that parents/carers are aware of the schools online safety (e-Safety) ethos and are actively engaged in supporting the school. Schools should be using their AUP as a way of engaging with families and by sharing the AUP with parents/carers when their children start attending the school, this can help establish a shared responsibility and approach to online safety. Additional statements may be required depending on individual settings use of technology by parents/carers, for example if formal/informal communication channels such as email or text messages are utilised by parents/carers.

Many schools will wish to request that children and parents/carers return a slip to say they have read the pupil AUP. Schools will need to decide whether or not they wish parents to sign to acknowledge the AUP on behalf of, or alongside their child, and this will depend on the age and ability of pupils. Some schools will chose to obtain parents acknowledgement regarding AUPs on an annual basis, others at point of admission and transition between key stages and this may depend on the school type as well as administration and leadership decisions. Some schools may choose to request that parents/carers read and sign the pupil AUP to show their agreement with the school AUP (be aware that this is different to an acknowledgment). Schools must be aware that if parents/carers refuse to sign and agree the AUP then this can cause problems as children will need to use the internet in order to access the curriculum. All schools will need to ensure they have a robust process in place to manage and record parental responses and also to engage with parents who do not respond.

It is recommend that parental awareness and engagement with the pupil AUP is achieved by including the pupil AUP and highlighting safe practice and expectations as part of the Home School Agreement. Parents/carers will need to be made aware (such as through the Home School Agreement) that the school will take every effort and all reasonable precautions to ensure that children cannot access inappropriate or illegal content whilst using the internet via school provided systems (including school provided Wi-Fi), however this cannot always be possible due to the dynamic nature of the internet. Schools may wish to reassure parents of the reasonable precautions they will take to limit this risk, such as appropriate supervision of children.

Schools could also use the Home School agreement to ensure parents are aware of the schools expectations of online conduct for the whole school community. Schools may wish to include specific statements such as "*We are aware of the schools Acceptable Use and online safety (e-Safety) policies and will support the school's approach to online safety (e-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 school community*".

Some schools are additionally requesting that parents themselves sign a specific AUP for parents/carers which highlights how the school and family will work together to keep the whole school community safe online. A sample is included within this document for schools to adapt if this approach is preferred.

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 (e-Safety) education begins as soon as children begin using technology.

Schools and settings will need to decide which approach for parental engagement best suits their school community and the leadership team should carefully consider which approach would be the most applicable.

Pupils Acceptable Use Policy: Sample Statements

The following statements are provided as suggestions and guidance only and it is recommended that schools write their own AUP to reflect the needs and abilities of their pupils/community, the technology available and the schools online safety (e-Safety) ethos. Where possible and appropriate, children and young people should be directly involved in this process.

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

Larger versions of the posters available for use to reinforce the schools expectations regarding pupils' acceptable use of technology can be found at www.kelsi.org.uk (via the e-Safety section) and www.eiskent.co.uk

Possible Statements for Early Years and KS1 (0-7)

- I only use the internet when an adult is with me
- I only click on links and buttons 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 e.g. tablets, cloud computing, pupil owned devices
- I know that if I do not follow the rules then:
    - List school 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

EYFS and KS1 shortened version (for use on posters etc.)

- 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

Possible Statements for KS2 Pupils (7-11)

- 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 my 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 by schools)
- I know that not everything or everyone online is honest or truthful and 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
- I only talk with and open messages from people I know and I only click on links if I know they are safe
- 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
- I only send messages which are polite and friendly
- 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 peoples files or information
- I will only post pictures or videos on the Internet if they are appropriate and if I have permission
- I will only change the settings on the computer if a teacher/technician has allowed me to
- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.
- 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
- I know that my use of school devices/computers and Internet access will be monitored
- Schools should include specific information and expectations relating to the use of devices and technology in school e.g. tablets, laptops, cloud computing, pupil owned devices, shared file storage areas.
- I know that if I do not follow the rules then:
    - List school sanctions
- 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 etc)
- I have read and talked about these rules with my parents/carers
- If I am aware of anyone being unsafe with technology then I will report it to a teacher
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about keeping safe online

KS2 Shortened version (for use on posters etc)

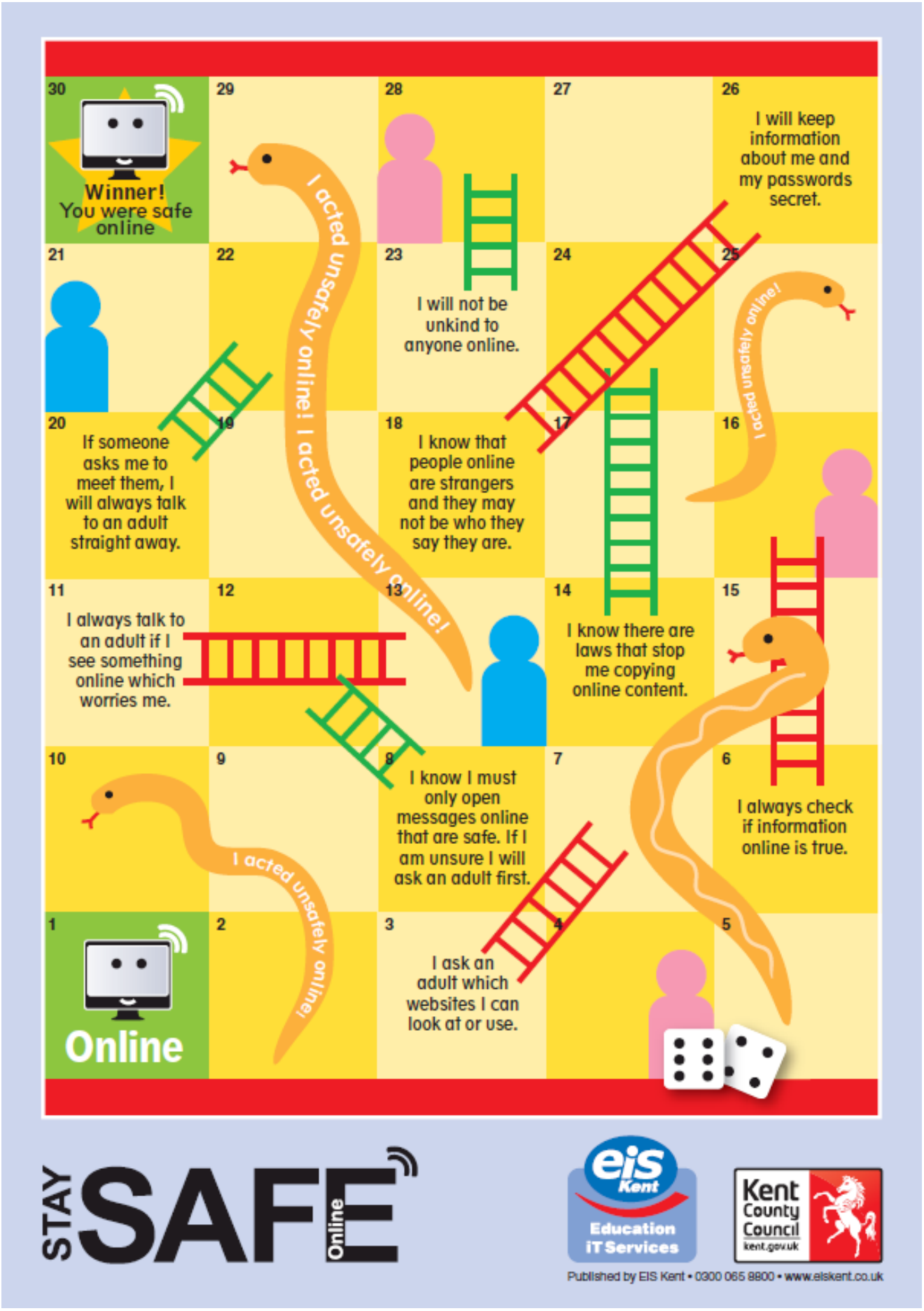
- I ask an adult which websites I can use
- I will not assume information online is true
- I know there are laws that stop me copying online content
- I know I must only open online messages that are safe and if I'm unsure then I won't open it without speaking to an adult first
- I know that people online are strangers and they may not always be who they say they are
- If someone online suggests meeting up then 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

Alternative KS2 Statements

- 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 / CD ROMs from outside of school I will always give them to my teacher so they can be checked for viruses and content, before opening a file.
- 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 e-mail, 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.

With thanks to Kingsnorth Primary School

KS2 Acceptable Use Poster



Possible Statements for KS3/4/5 Students (11-18)

- 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 then 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 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 at all times
- 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 (Be aware that 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 then 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
- Schools should include specific information and expectations relating to use of devices in school e.g. tablets, cloud computing, pupil owned devices e.g. "If I am given permission by a member of staff to use a personal device in school then I will abide by these rules whilst using the device(s) in school."

KS3/4/5 Shortened version (for use on posters in Classrooms etc)

Responsibility

- 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

Privacy

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

Respect and Reputation

- 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

Safe and 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
- I know my online actions have offline consequences

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

Additional/Brief statement for KS3/4/5

At xxx School we want to ensure that all members of our community are safe and responsible users of technology.

We will support pupils to…

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

KS3/4 Acceptable Use Poster

STAY **SMART!** online ONLINE Online Online

I must respect the school's systems and equipment. If I can not be responsible I will lose the right to use them.

RESPONSIBILITY

I must check the reliability of online content, in case it is untrue.

Privacy

I will keep my password and personal information secret.

I know I must always check that my privacy settings are confidential.

I know that my internet use is monitored to protect me.

I am aware that copyright laws exist.

I know that my online actions may have offline consequences.

I know that it can be a criminal offence to hack accounts and systems or to send threatening and offensive messages.

I will always think before I post as once I upload content it can become public and difficult to delete.

I will not use technology to be unkind to people.

REPORT

I know that people online are not always who they say they are. I will always talk to an adult before meeting any online contacts.

If anything happens online which makes me feel worried or uncomfortable, I will speak to an adult I trust or visit ***www.thinkyouknow.co.uk***.

eis Kent Education iT Services

Kent County Council kent.gov.uk

Published by EIS Kent • 0300 065 8800 • www.eiskent.co.uk

Possible Statements for Children with Special Educational Needs and Disabilities

(These statements are based on ability levels rather than age)

Children and Young People 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

Children 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 then I tell a grown up

Children and Young People 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 then I tell an adult

Insert School Logo Here

Sample Parent/Carers Acceptable Use Policy Statements

- I have read and discussed the Acceptable Use Policy (attached) with my child
- I know that my child will receive online safety (e-Safety) education to help them understand the importance of safe use of technology and the internet, both in and out of school.
- I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons and to safeguard both my child and the schools systems. This monitoring will take place in accordance with data protection and human rights legislation.
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.
- 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
- I understand that if my child does not abide by the school Acceptable Use Policy then sanctions will be applied in line with the schools behaviour and anti-bullying policy (include as appropriate). If the school believes that my child has committed a criminal offence then the Police will be contacted
- I, together with my child, will support the school's approach to online safety (e-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
- I know that I can speak to the school Online Safety (e-Safety) Coordinator (Name), my child's teacher or the Head Teacher if I have any concerns about online safety (e-Safety)
- 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
- I will visit www.thinkuknow.co.uk/parents, www.nspcc.org.uk/onlinesafety, www.internetmatters.org www.saferinternet.org.uk and www.childnet.com for more information about keeping my child(ren) safe online
- 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 the Parent Acceptable Use Policy.

Child's Name…… Class……

Parents Name…….....Parents Signature……

Date……..

Note: Please be aware that if parents/carers refuse to sign and agree the AUP then this can cause issues as children will need to use the internet in order to access the curriculum. Schools must have a robust process in place to manage and record parental responses and also to engage with parents who do not respond. Alternatives include highlighting online safety (e-Safety) within the Home School Agreement and an acknowledgement form for the AUP.

Insert School Logo Here

Use of Cloud Systems Permission Form

Schools that use cloud hosting services may be required to seek parental permission to set up an account for pupils / students. Cloud systems such as Google Apps for Education services www.google.com/apps/intl/en/terms/education_terms.html may require that schools obtain 'verifiable parental consent' for children to be able to use the system and services. Schools may wish to incorporate this into their standard acceptable use consent forms. Schools will need to review and amend the section below, depending on which cloud hosted services are used. The Department for Education has published advice and information regarding Cloud (educational apps) software services and the Data Protection Act here: https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

The school uses Google Apps for Education for pupils and staff. This consent form describes the tools and pupil responsibilities for using these services.

The following services are available to each pupils and hosted by Google as part of the school's online presence in Google Apps for Education (amend as appropriate as not all schools will use all options/apps):

- **Mail** - an individual email account for school use managed by the school
- **Calendar** - an individual calendar providing the ability to organize schedules, daily activities, and assignments
- **Docs** - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office
- **Sites** - an individual and collaborative website creation tool

Using these tools, pupils collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of school learning experiences, and working in small groups on presentations to share with others.

(Insert specific school action and details regarding safeguarding measures being taken by the school, including data protection, pupil training, supervision etc)

The school believes that use of the tools significantly adds to your child's educational experience.

As part of the Google terms and conditions we are required to seek your permission for your child to have a Google Apps for Education account:

Use of Cloud Storage Systems – Parental Consent

Child's Name……. Class……

Parents Name…….....

Parents Signature……..

Date…….

Optional Form.
This form was originally created and has been kindly shared by the South West Grid for Learning: www.swgfl.org.uk
This form should be used in accordance with DfE Guidance: https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

Sample Letter for parents/carers

Dear Parent/Carer

All pupils use computer facilities including 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
- Internet which may include search engines and educational websites
- School learning platform/intranet
- Email
- Games consoles and other games based technologies
- Digital cameras, web cams and video cameras
- Recorders and Dictaphones
- Mobile Phones and Smartphone's

(NAME) school recognise the essential and important contribution that technology plays in promoting children's learning and development and offers a fantastic range of positive activities and experiences. However we also recognise there are potential risks involved when using online technology and therefore have developed online safety (e-Safety) policies and procedures alongside the schools safeguarding measures. (School may wish to include specific details such as filtering, monitoring and use of personal devices).

The school takes responsibility for your child's online safety very seriously and, as such, we ensure that pupils are educated about safe use of technology and will take every reasonable precaution to ensure that pupils cannot access inappropriate materials whilst using school equipment. (School should include specific details about precautions taken, such as use of devices, appropriate supervision, education and curriculum approaches etc. The school must then ensure that appropriate precautions are in place) However no system can be guaranteed to be 100% safe and the school cannot be held responsible for the content of materials accessed through the internet and the school is not liable for any damages arising from use of the schools internet and ICT facilities.

Full details of the school's Acceptable Use Policy and online safety (e-Safety) policy are available on the school website (link) or on request.

We request that all parents/carers support the schools approach to online safety (e-Safety) by role modelling safe and positive online behaviour for their child and by discussing online safety with them whenever they access technology at home. Parents/carers can visit the school website's (link) for more information about the school's approach to online safety as well as to access useful links to support both you and your child in keeping safe online at home. Parents/carers may also like to visit www.thinkuknow.co.uk, www.childnet.com, www.nspcc.org.uk/onlinesafety, www.saferinternet.org.uk and www.internetmatters.org for more information about keeping children safe online

Whilst the school monitors and manages technology use in school we believe that children themselves have an important role in developing responsible online behaviours. In order 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 and that you and your child discuss the content and return the attached slip. 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.

Should you wish to discuss the matter further, please do not hesitate to contact the school online safety Coordinator (name) or myself.

(Additional Paragraph for Early Years/KS1/SEN)
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.

Yours sincerely,
Headteacher

Insert School Logo Here

Parent/Carer Acceptable Use Policy Acknowledgement Form

Pupil Acceptable Use Policy – xxxx School Parental Acknowledgment

I, with my child, have read and discussed xxxxx school 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 all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task. I understand that the school will take all reasonable precautions to reduce and remove risks but cannot ultimately be held responsible for the content of materials accessed through the Internet.

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 e-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……..

Insert School Logo Here

Sample Letter for Students (KS3/4/5)

Dear xxxx

All students at our school use computer facilities including Internet access as an essential part of learning and fun in today's modern British Society. You 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
- Internet which may include search engines, social media and educational websites
- School learning platform/intranet
- Email
- Games consoles and other games based technologies
- Digital cameras, web cams and video cameras
- Recorders and Dictaphones
- Mobile Phones and Smartphone's

At (NAME) school 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 involved when using online technology. 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 such as filtering, monitoring and use of personal devices etc.)

At xxx School 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 school resources and technology safely, carefully and responsibly
- Be kind online and help us to create a school community that is respectful and caring, on and offline
- Be safe and be sensible online and always know that you can talk to a trusted adult if you need help

We request that you and your family read the school Acceptable Use Policy and return the attached slip.

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 look forward to helping you become a positive and responsible digital citizen.

Yours sincerely,

Headteacher

Pupil Acceptable Use Policy – xxxx School Pupil Response

I, with my parents/carers, have read and discussed the xxxxx school Pupil Acceptable Use Policy.

Child's Name……. Signed……..

Class…… Date……..

Parents Name…….....Parents Signature…….

Date…….

Insert School Logo Here

Sample Letter for Staff

Please note this letter does NOT replace a Staff AUP

Dear xxxxx

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 the Online safety (e-Safety) Coordination/ Designated Safeguarding Lead /Manager (name).

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 e.g. 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, www.e-safety.org.uk and www.gov.uk/government/publications/preventing-and-tackling-bullying. Staff can also visit or contact the Professional Online safety Helpline www.saferinternet.org.uk/about/helpline for more advice and information on online professional safety.

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

Yours sincerely,

Headteacher

Additional content for staff 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 then 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 at all times 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 head teacher of any concerns such as criticism or inappropriate content posted online.

Insert School Logo Here

xxxx Staff Acceptable Use Policy 2015

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

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate 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 – include school information and requirements e.g. 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 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 (schools might wish to attach their Data Security Policy). Any images or videos of pupils will only be used as stated in the school image use policy (schools may wish to attach a copy of the 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 (Schools might wish to attach a copy of the policy or include specific expectations).

11. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead (name) and/or the Online Safety Coordinator (name if different) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to (name) Designated Safeguarding Lead (name) and/or the Online Safety Coordinator (name if different) and/or the designated lead for filtering (name) as soon as possible. (Schools may wish to attach a reporting flowchart).

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 ICT Support Provider/Team/lead (named contact) as soon as possible. (Schools may wish to provide more specific details about accessing technical help here).

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 e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.

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 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, then I will raise them with the Designated Safeguarding Lead (name) and/or the Online Safety Coordinator (name if different) or the Head Teacher.

18. Schools will need to include specific details and expectations regarding safe practice relating to the specific use of technology within school e.g. 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.

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

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

Accepted by: ……. Print Name: ……..

Insert School Logo Here

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 are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy. This is not an exhaustive list and 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 pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. 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. (please note this statement is only required if visitors/volunteers have access to data)

2. 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.

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 at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.

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, then I will raise them with the Designated Safeguarding Lead (name) or the Head Teacher.

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

I have read and understood and agree to comply with the Visitor /Volunteer Acceptable Use Policy.

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

Accepted by:…….. ……Date: ……..

Insert School Logo Here

Wi-Fi Acceptable Use Policy

For those using school Wi-Fi

Schools/settings may wish to use a paper or electronic AUP for guest access of Wi-Fi by members of the community. Schools may choose to require that visitors agree to an on screen electronic AUP as part of the process of accessing the Wi-Fi. This template is provided for schools 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.

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 (state purpose e.g. education use only) Schools should include any include information about time limits, passwords, security etc.

1. The use of ICT devices falls under xxxx school's Acceptable Use Policy, online safety (e-Safety) policy and behaviour policy (any other relevant policies e.g. data security, safeguarding/child protection) which all students/staff/visitors and volunteers must agree to, and comply with.

2. 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.

3. 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.

4. 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).

5. 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. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the school harmless from any claim or loss arising out of, or related to, any such instance of hacking or other unauthorized use or access into my computer or device.

6. 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.

7. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.

8. 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.

9. I will not attempt to bypass any of the schools security and filtering systems or download any unauthorised software or applications.

10. 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.

11. 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.

12. I will report any online safety (e-Safety) concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (name), the Online Safety (e-Safety) Coordinator (name) and/or the designated lead for filtering (name) as soon as possible.

13. If I have any queries or questions regarding safe behaviour online then I will discuss them with the Online safety (e-Safety) Coordinator (name) or the Head Teacher.

14. 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: …….

Insert School Logo Here

Social Networking Acceptable Use Policy

For parents/volunteers running school/setting social media accounts e.g. PTA groups and committees

1. As part of the school's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the school's approach to online safety (e-Safety). I am aware that (tool using e.g. Facebook, Twitter) a public and global communication tool and that any content posted on the site/page/group may reflect on the school, its reputation and services. 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.

2. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Designated Safeguarding Lead (name) or the head teacher. The head teacher (or other appropriate member of senior 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 e.g. Facebook, Twitter) 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.

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

4. I will follow the school's policy regarding confidentially and data protection/use of images. I will ensure that I have written permission from parents/carers or the school before using any images or videos which include members of the school community. 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 and these will be for the sole purpose of inclusion on (tool using e.g. Facebook, Twitter) and will not be forwarded to any other person or organisation.

5. I will promote online safety in the use of (tool using e.g. Facebook, Twitter) and will help to develop a responsible attitude to safety online and to the content that is accessed or created.

6. 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 and/or school management team will have full admin rights to the account.

7. 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.

8. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the Designated Safeguarding Lead (name) and/or head teacher immediately.

9. I will ensure that the (tool using e.g. Facebook, Twitter) is moderated on a regular basis as agreed with the Designated Safeguarding Lead (name) and/or head teacher.

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 and the safe use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the head teacher.

11. 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 head teacher.

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

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

Accepted by: …….. Print Name: ……..

Insert School Logo Here

Staff Social Networking Acceptable Use Policy

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 (e-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. 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.

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

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

4. 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. These will be for the sole purpose of inclusion on (tool using e.g. Facebook, Twitter) and will not be forwarded to any other person or organisation.

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

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

7. Where it believes unauthorised and/or inappropriate use of the (tool using e.g. Facebook, Twitter) or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.

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

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

10. I will ensure that the (tool using e.g. Facebook, Twitter) site/page is moderated on a regular basis as agreed with the school Designated Safeguarding Lead.

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

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

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

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

Accepted by: ……. Print Name: ……

Further Information

Kent Resources

- Kent Schools and settings can consult with the Education Safeguarding Adviser (Online Protection) and e-Safety Development Officer via: esafetyofficer@kent.gov.uk or 03000 415797.
- Online safety training is available for education settings via CPD Online www.kentcpdonline.org.uk and KSCB www.kscb.org.uk
- Kent County Council's Online Safety (e-Safety) Materials for schools and settings can be found at www.kelsi.org.uk
- "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. The document can be downloaded from www.e-safety.org.uk

Other Resources

- "Supporting School Staff" is an essential document to help staff understand how to protect themselves online created by Childnet International and DfE: http://www.digizen.org/resources/school-staff.aspx
- The UK Safer Internet Centre's Professional Online safety Helpline offers advice and guidance around e-Safety issues for professionals who work with children and young people in the UK. The helpline provides support with all aspects of digital and online issues such as social networking sites, cyber-bullying, sexting, online gaming and child protection online. Staff can contact the helpline via 0844 381 4772, helpline@saferinternet.org.uk or can visit www.saferinternet.org.uk/helpline for more information.
- 360 Degree Safe tool is an online audit tool for schools to review current practice: http://360safe.org.uk/
- 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. www.swgfl.org.uk/onlinecompass

- Department for Education
    - Keeping Children Safe in Education 2016 https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
    - Cloud Computing: https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act
    - Teaching Standards: https://www.gov.uk/government/collections/teachers-standards.
    - Preventing and Tackling Bullying: https://www.gov.uk/government/publications/preventing-and-tackling-bullying

Additional links and resources to support safe and responsible use of technology

- UK Safer Internet Centre: www.saferinternet.org.uk
- Think U Know: www.thinkuknow.co.uk
- Childnet International: www.childnet.com
- CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
- NSPCC: www.nspcc.org.uk/onlinesafety
- Digital Literacy Scheme of Work: www.digital-literacy.org.uk
- South West Grid for Learning: www.swgfl.org.uk
- Internet Matters: www.internetmatters.org
- The Parent Zone: www.theparentzone.co.uk

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.