WMnet E-safety

Acceptable Use Policies for Schools

As the use of online services and resources grows, so has awareness of the risks and potential dangers which arise from the use of communications technology and the internet. Those risks are not confined to the use of computers; they may also arise through the use of other devices eg games consoles and mobile phones.

There is an expectation that schools will have in place appropriate policies and strategies to promote the safety of learners in their care both when they are in the school and when they are elsewhere.

Part of the apparatus for promoting e-safety is likely to be a set of acceptable use policies (AUPs). The enclosed drafts are intended to be read as notes towards the contents of schools' acceptable use policies; they are intended to act as a skeleton for a school's policies; perhaps to form the basis of the text which appears on screen when a user logs on to a school's learning platform or VLE. They could also be used and have been used as teaching aids for school age learners and adults.

For more detailed guidance on e-safety, please refer to the following sites:

www.becta.org.uk – Becta is the main agency for communicating with schools on behalf of DCSF on e-safety matters.

www.thinkuknow.co.uk - This website, developed by the Child Exploitation and Online Protection (CEOP) Centre, provides information for young people on how to stay safe on line

www.childnet-int.org - Childnet International's Kidsmart website has a section for young people aged 11 plus, dealing with mobiles, filesharing, chat, trackback (for example, digital footprints) and privacy.

www.ceop.police.uk - The Child Exploitation and Online Protection (CEOP) Centre is dedicated to eradicating the sexual abuse of children.

www.getsafeonline.org – Advice on data security and staying safe on line

Schools will also need to ensure that their policies and practices are consistent with local arrangements and policies implemented by their Local Safeguarding of Children Board and local authority Directorate of Children's Services.

The following AUP guidance drafts are enclosed

1. AUP for younger learners in KS1
2. AUP for learners in KS2 and KS3
3. AUP for learners in KS3 and above
4. AUP for adults working with young people
5. AUP for schools and governors

These documents draw upon work done in Dudley, Kent, Islington, South West Grid for Learning and a number of other areas.

AUP Guidance notes for learners in KS1

I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger

Anything I do on the computer may be seen by someone else.

I am aware of the CEOP report button and know when to use it.

AUP Guidance notes for learners in KS2 and KS3

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only use, move and share personal data securely
- only visit sites which are appropriate
- work in collaboration only with people my school has approved and will deny access to others
- respect the school network security
- make sure all messages I send are respectful
- show a responsible adult any content that makes me feel unsafe or uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not use my own mobile device in school unless I am given permission
- only give my mobile phone number to friends I know in real life and trust
- only email people I know or approved by my school
- only use email which has been provided by school
- obtain permission from a teacher before I order online
- discuss and agree my use of a social networking site with a responsible adult before joining
- always follow the terms and conditions when using a site
- always keep my personal details private. (my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult before I share images of myself or others
- only create and share content that is legal
- never meet an online friend without taking a responsible adult that I know with me

I am aware of the CEOP report button and know when to use it.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

AUP Guidance notes for learners in KS3 and above

The policy aims to ensure that any communications technology is used without creating unnecessary risk to others.

I agree that I will:

- only use, move and share personal data securely
- respect the school network security
- set strong passwords which I will not share
- not use my own mobile device in school unless I am given permission
- respect copyright and the intellectual property rights of others
- only create and share content that is legal
- always follow the terms and conditions when using a site
- only visit sites which are appropriate
- discuss and agree my use of a social networking site with a responsible adult before joining
- obtain permission from a teacher before I order online
- only use approved email accounts
- only use appropriate content which I have permission to use
- only communicate online with trusted users
- never meet an online friend without taking a responsible adult that I know with me
- make sure all messages/posts I send are respectful
- not respond to or forward any inappropriate message or content
- be cautious when sharing personal contact information
- only communicate electronically with people I know or have been approved by my school
- report unsuitable content or activities to a member of staff

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I am aware of the CEOP report button and know when to use it.

Continued…

I agree that I will not:

- visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
- pornography (including child pornography)
- promoting discrimination of any kind
- promoting violence or bullying
- promoting racial or religious hatred
- promoting illegal acts
- breach any Local Authority/School policies, e.g. gambling
- do anything which exposes children in my care to danger
- any other information which may be offensive to others
- forward chain letters
- breach copyright law
- do anything which exposes others to danger

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

AUP Guidelines for any adult working with learners

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users whilst supporting learning.

Please check that this is compatible with your local authority policies before using this AUP.

I agree that I will:

- only use, move and share personal data securely
- respect the school network security
- implement the schools policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources
- respect the copyright and intellectual property rights of others
- only use approved email accounts
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site.
- only give permission to pupils to communicate online with trusted users.
- use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- not use or share my personal (home) accounts/data (eg Facebook, email, ebay etc) with pupils
- set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- report unsuitable content and/or ICT misuse to the named e-Safety officer
- promote any supplied E safety guidance appropriately.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Continued…

I agree that I will not:

- visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
- pornography (including child pornography)
- promoting discrimination of any kind
- promoting violence or bullying
- promoting racial or religious hatred
- promoting illegal acts
- breach any Local Authority/School policies, e.g. gambling
- do anything which exposes others to danger
- any other information which may be offensive to others
- forward chain letters
- breach copyright law
- use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission
- store images or other files off site without permission from the head teacher or their delegated representative.

I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.

I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

AUP Guidance notes for schools and governors

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to supporting learning without creating unnecessary risk to users.

Please check that this is compatible with your local authority policies before using this AUP.

The governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-Safety Coordinator and a named governor takes responsibility for e-Safety
- an e-Safety Policy has been written by the school, building on the LSCB e Safety Policy and BECTA guidance
- the e-Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology (using the Self-Review Framework) to establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff