

Next Generation Learning

E-Safety Guidance for Schools

Contents

Page 2	Context and Introduction
Page 3	The Need for an eSafety Policy
Page 4	School Acceptable Use Policies
Page 5	Acceptable Use agreements
Page 6	Who Writes the Policy
Page 6	Governing Body Responsibilities
Page 7	Parental Involvement
Page 6	Acceptable Use
Page 8	Reviewing the AUP Policy
Page 8	Key Sections of an Acceptable Use Policy
Page 8	Using the Technologies Safely
Page 9	Internet safety skills development for staff
Page 9	Internet safety skills development for pupils
Page 10	Impact of Social Networking Sites in School
Page 11	School Websites and Images of Children and Staff
Page 11	Acceptable Use of ICT Facilities within the School Library
Page 11	Community Use
Page 12	Areas of teaching
Page 14	Responding to Incidents of Misuse
Page 15	Appendices – examples of acceptable use agreements
Page 17	eSafety checklist
Page 21	References and Resource Links

Context

Internet access is an important learning tool for schools. Access to the internet and a wide range of resources for learning is considered essential and plays a major role in any learner's development. Schools need to have good management processes in place to ensure safe and effective use of the Internet by staff and pupils.

A school will need to discuss with its staff, pupils, governing body and parents when developing and implementing their policy for Internet access. Policies should be in place for all users of ICT systems and the Internet – these policies should explicitly encompass staff and other adults working or visiting the school as well as learners. This guidance will support the process.

Introduction

Use of the Internet is continually expanding and has become an important part of learning and communication. The Internet brings pupils into contact with a wider range of information, the scope and nature of which may or may not be appropriate for the pupil.

Using the Internet is now an everyday occurrence for most adults and children. With ever expanding new technologies such as blogs (online diaries), social networking spaces, online chat and mobile phones children are using technology in a way never seen before. The increased use of technology at school and home also exposes children to a number of risks and dangers. In its simplest form e-Safety is about ensuring children use new technologies in a way which will keep them safe without limiting their opportunities for creation and innovation.

The statutory curriculum expects pupils to learn how to locate, retrieve and exchange information using ICT. When planning the curriculum, teachers need to prepare for and make use of communications technology i.e. web-based resources, the use of the schools Learning Platform, email and other web based technologies such as blogs. Access to life-long learning and enhancement of employment requires learners to be capable in the use of ICT and there is a need to develop skills in their use.

Through the use of the Internet based activities those adults supporting learning within a school environment are able to enrich the range of opportunities and resources available to learners. They should be aware of the risks as well as the opportunities presented.

A school's Internet Access Policy is part of the school's ICT development plan and should relate to other policies including those for behaviour, citizenship and personal, social and health education.

Schools are encouraged as part of their self evaluation to review ICT using the Becta self review matrix. <http://selfreview.becta.org.uk/>

The publication by Becta, '**Developing whole-school policies to support effective practice**' is recommended as a reference guide in developing a **school e-safety policy**.

<http://publications.becta.org.uk/display.cfm?resID=25934>

The Need for Internet Access Policy

There is evidence that the digital world is having an impact on the welfare of children and young people and those that work with them. There are related risks and these impact upon policy development and training in health care, schools and education, youth work, policing, community safety, social care, human resources and Information Communication Technology (ICT).

The Byron review - makes a case for "empowering young people to manage risks and make the digital world safer" and identifies on-line risks as being problematic because of their anonymity and ubiquity.

The response of Ofsted to the Byron review suggests schools are unaware whether their e-safety measures are effective or not. The new Ofsted framework for inspection will take account of a schools child protection policy including e-safety.

References:

http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrssi/

<http://www.tda.gov.uk/teachers/hottopics/esafety.aspx>

<http://www.digizen.org/cyberbullying/fullguidance/>

<http://www.nya.org.uk/information/111564/youthworkandsocialnetworking/>

The Internet is managed by a worldwide, non-statutory collaboration of independent agencies that serve both young and adult audiences. Without appropriate measures, access to unsuitable materials would be possible and security compromised. An Internet Access Policy will help to ensure that Internet supports school's educational aims, that responsibilities to pupils are met and that safety and security requirements are satisfied. In addition, the DCSF requires that a school's ICT development plan must set out their policy to protect pupils from access to undesirable materials.

Although teachers will have heard about the inappropriate aspects of the Internet, few will have had opportunities to discuss the issues in detail. The writing of the policy provides such an opportunity and the agreed policy produced is more likely to be implemented effectively. When writing the policy both appropriate and inappropriate behaviours should be covered. For adult users of the school's resources it can be that inappropriate behaviour can jeopardise the safety of children or the security of their information and the policy writers need to be mindful of this when creating the policy.

An acceptable use policy must be wide-ranging. It must consider both the fixed and mobile internet; technologies provided by the school (such as computers, laptops, webcams and digital video equipment); and technologies owned by pupils and staff, but brought onto school premises (such as mobile and camera phones, personal digital assistants (PDAs), and portable media players). It should be flexible enough to deal with new and emerging technologies, but should also recognise the important educational and social benefits of such tools.

This guidance is intended to help the development of a school's AUP without bypassing the essential debate with pupils, students, staff, parents and the Governing Body.

School Acceptable Use Policies

Creating a safe learning environment must include effective ICT policies and procedures. Acceptable Use Policies are documents explaining the ways in which ICT can and cannot be used by all members of the school community. They should be personalised by individual schools and be regularly up dated as part of school review processes and as practice and technologies develop. They should be followed by all pupils, staff and other persons connected to the school, they should reflect other codes of conduct used in the school.

The Purpose of the Acceptable Use Policy is to Set Out:

- for parents, pupils, staff and the Governing Body the steps taken within Wakefield LA and in school, to ensure the safety of children when using the Internet, email and related technologies
- the school's expectations for the behaviour of children whilst online and using the Internet, email and related technologies.
- how the school will ensure that pupils, parents, staff and others understand the benefits and the dangers associated with the Internet, email and related technologies so that they are able to use ICT safely at school, home and elsewhere.

It is possible to obtain a ready-made Acceptable Use Policy for from a number of sources, including the Internet itself. However, it is advisable that each school sets aside time to develop their own policy. Early feedback from schools, having undergone Safeguarding inspections by Ofsted, report that it is the process that is the essential element. This will ensure that members of your staff have the opportunity to talk through the issues surrounding the Internet in education.

An acceptable use policy should extend to all young children and the professionals working with them regardless of whether this is in an educational, home, or wider community setting. The NEN website (www.nen.gov.uk) contains a number of useful resources including an audit tool that should assist organisations in assessing their e-safety status.

Acceptable Use Agreements

Clear guidance is needed for young people and all professionals who come into contact with them on what is acceptable use. An acceptable use agreement is intended to remove any ambiguity and ensure that all young people and the professionals who work with them are protected. The appendix provides some sample acceptable use agreements which schools are able to adapt for their use. It is important to stress these are for guidance and should not replace the need for discussion with pupils, staff, parents and Governing Bodies in developing an Acceptable Use Policy Document.

The sample acceptable use agreements maybe a useful resource in discussions with staff, pupils and parents.

- **Acceptable Use Agreements for Staff (appendix 1)**

It is important that schools provide guidelines for staff on how they may use the school's ICT facilities. This will help to protect staff and promote understanding amongst staff.

- **Acceptable Use Agreements for Pupils (appendix 2 and 3)**

While no technological solution can be 100 per cent effective in guaranteeing safety when using the internet and related technologies, technology can help to minimise the risks to pupils, particularly when supported by a clear acceptable use policy and appropriate internet safety education. It is recommended that pupils are involved in the creation of school internet acceptable use agreements, possibly through pupil representation on the school's internet safety policy team or through PSHCE activities.

The acceptable use agreement/guidelines must be appropriate to the pupil's age and prior exposure to ICT. The examples in the appendix are for guidance.

Who Writes the Acceptable Use Policy?

The Headteacher may direct a member SMT to develop/coordinate the development of an Internet Access Policy and in consultation with other staff or interested parties. Due to the nature of the content of the policy and potential impact in disciplinary matters affecting staff or pupils, it is essential that the school's Governing Body are aware of the policy and its content and have agreed its implementation. It is vital that all users are aware of the policy and that they have accepted it before they access a school's ICT system.

Headteachers, with the support of governors, should take a lead in embedding effective e-safety practices into the culture of the school, while a designated senior management role of e-safety coordinator can assist with co-ordinating e-safety activities on a day-to-day basis. This member of staff should act as a central point of contact for all e-safety issues within the school, ensuring that policies are in place, current and adhered to, instances of breaches and misuse are monitored and reported through an incident reporting process. This will help inform staff and ensure that all staff receive relevant information about emerging issues.

Governing Body Responsibilities

Governing bodies have statutory responsibilities for child protection and health and safety, and elements of these will include internet safety.

Suggested Responsibilities for Governing Bodies

- Developing an awareness of the issues and risks of using ICT in schools, alongside the benefits, particularly with regard to the internet and other communications technologies. Consider appointing an e-Governor, that is a governor with specific responsibility for ICT, and ensure that internet safety is included as part of the regular review of child protection and health and safety policies.
- Developing an understanding of existing school policies, systems and procedures for maintaining a safe ICT learning environment and supporting the headteacher (or designated member of staff) in implementing these, including ensuring access to relevant training for all school staff.
- Supporting the headteacher (or designated member of staff) in developing an appropriate strategy and plan for dealing with the media should serious incidents occur. In such an instance, it is likely that the chair of the governing body will be approached by the press for comment.
- Ensuring that appropriate funding is authorised for internet safety solutions, training and other activities as recommended by the headteacher (or designated member of staff), as part of the wider remit of the governing body
- with regard to school budgets.

- Promoting internet safety to parents, and providing updates on internet safety policies within the statutory 'security' section of the annual report. Becta has been commissioned by the DCSF to produce a free series of ICT Guides for Governors.

<http://www.becta.org.uk/leaders/governors>

Parental Involvement

Parents and carers should be involved on internet safety issues, and, where possible, should be consulted in the development of the school policy.

It is essential that schools communicate with parents, informing them of the steps the school takes to ensure a safe ICT learning environment, and making them aware of the expected behaviours when using ICT just as there are standards of behaviour for other activities in school.

Communication with parents about ICT use in school, through the acceptable use policy or through special meetings in school reinforces the safety messages taught in school and can help alleviate some of the fears associated with the use of new technologies.

While there is no statutory requirement for parents to sign acceptable use policies, schools should consider a signed acceptable use form as key part of the administrative processes each year or as part of the home–school agreement. Older pupils/students should agree to the rules themselves. Clearly, the language must be appropriate to the age and understanding of the children.

Parents have a key role to play in the internet safety education of their children, through promoting internet safety at home. ICT offers the opportunity for children and their parents to learn together, and internet safety is a topic that can encourage home–school links. Schools should consider running a parent workshop/presentation on e-safety where key messages and safety guidance can be shared to help ensure consistency between safety guidelines in the home and the school.

Reviewing the AUP

Staff, pupils and the Governing Body of the school should be involved in the AUP creation. It is also important that there is regular review of the AUP by the all groups in schools.

- **Review Procedure**

1. There should be an on-going opportunity for Staff, pupils and the Governing Body to discuss with the person responsible any issue of eSafety that concerns them.
2. The policy should be reviewed every (12) months and consideration given to the implications for future whole school development planning.
3. The policy should be amended as new technologies are adopted or Central Government change the orders or guidance in any way

Key Sections of an Acceptable Use Policy

Becta have produced a document that supports the development of an Acceptable Use Policy and is highly recommended. It covers all aspects of policies that schools should have in place.

E-safety: Developing whole-school policies to support effective practice (follow the above link)

Using the Technologies Safely

In discussing the safe and appropriate use of technologies this should include technologies that may not necessarily be used within the school environment but likely outside school. Technologies to consider include instant messaging, webcams, chat rooms, email, recognising and dealing with spam and phishing, portable devices such as mobile phones/smart phones, video and peer-to-peer networking.

When assessing the potential risks in the use of images of pupils, the most important factor is the potential of inappropriate use of images of children. Staff training is required to support internet safety education and it is important to consider at what stage and where in the curriculum this might take place. It may not be best to leave this to just the ICT department or staff in school.

Internet safety skills development for staff

Internet safety awareness should be based on an ongoing programme of education within the school, and staff should not be excluded. In order to assist children and young people to stay safe when using the technologies, it is vital that staff are aware of the issues, both existing and emerging.

Staff should receive information and training on internet safety issues and new and emerging technologies on a regular basis. This training should be tailored to their particular role in the school (for example, a network manager will need very different training from a classroom teacher, who in turn will require different training from the child protection liaison person)

Internet safety skills development for pupils

Teachers are bound by a duty of care. As part of this duty it is important to raise awareness in children and young people of the risks associated with inappropriate content and on managing any contact via the internet

It is essential that all pupils are taught the relevant skills and strategies to remain safe when using the internet and related technologies. This may be as discrete internet safety lessons through PSHCE, as part of the ICT curriculum or indeed both. Clearly this would be supported across curriculum.

It is vital that opportunities are created for discussion, learning about risks, who to turn to and actions that pupils can take. It is not acceptable to simply issue an acceptable use agreement for parents/pupils to sign without any mediation.

Pupils will probably be aware of the impact of online bullying. This needs to be part of any skills development from the perspective of both the victim and the tormentor. It is vital they know where to seek help if affected by these issues.

Impact of Social Networking Sites in School

Introduction

There are several social networking sites, the most popular example is Facebook; others are BeBo and Connections on Yahoo Live Messenger.

A Facebook account allows you to keep in touch with 'friends' and other contacts allowing the sharing of pictures, notes etc. Care is required in using social network sites; whatever information is put on a Facebook page will be out on the Internet – possibly for ever. Whilst your profile can be set to be private so only your friends can see it, or public so anyone can view it; Facebook uses the term 'friend' very loosely and many people you don't know can be connected as friends and access anything you put on your page – and reuse it in anyway they wish. It's very important to not share private information such as address or phone numbers

The Blurring of School and Home

Facebook is used widely outside school and will be undoubtedly be used by many parents of children, support staff and teachers. Issues can arise when, for example, a teacher or a member of the support staff receives an invitation from a parent or pupil to become their 'friend'. Instances have arisen where teachers have shared their Facebook account with a parent who they are friendly with, resulting in pupils seeing pictures of the member of staff in potentially embarrassing situations out of work time.

It is therefore important that the school develops a policy to help protect staff as well as children from inappropriate use and connections through Facebook or similar social network accounts.

It is recommended that in general invitations from pupils or parents to teachers or support staff should be ignored/declined, keeping professional 'life' separate from social/home life. This needs to be established as school policy.

However, there will be instances where this will blur, for instance when a teacher is good friends with a member of the support staff who has a child in the school or where the friendship already exists. Clearly these specific personal situations will need to be brought to the attention of the Headteacher for declaration and guidance.

Teachers new to the profession should check their facebook or similar accounts for access level settings. This should also include the removal of redundant accounts.

Similar guidance is recommended concerning all personal information associated with staff, eg, mobile numbers, home and personal email addresses, msn and yahoo instant messenger IDs, Personal Twitter feeds etc.

For further guidance please refer to: **Guidance for Safer Working Practice for Adults who Work with Children and Young People in Education Settings', section 13**

School Websites and Images of Children and Staff

The school should establish clear policies to ensure that its website is effective, and does not compromise the safety of the pupils or staff. The website should be regularly checked to ensure that there is no content that compromises the safety of pupils or staff and is not in contravention of the data Protection Act. There should be a clear approval processes regarding the content that is loaded to the school's website. Pupils/students worked should be thoroughly checked if it is placed on the schools website.

Using images and digital video on school websites and Learning Platforms can be motivating for the pupils involved and provide a good opportunity to promote engagement with parents and carers.

When assessing the potential risks in the use of images of pupils, the most important factor is the potential of inappropriate use of images of children.

Schools therefore need to have a policy in relation to the use of images of pupils on the school's website or Learning Platform. The headteacher and governors will need to make decisions about the type of images they consider suitable and that appropriately represent the school.

For further guidance and suggested templates see:

www.gowild.wakefield.org.uk/dataprotection

Schools should also consider the way in which digital images and video are captured and stored within the school, guidelines should be established for the protection of both pupils and staff. These guidelines should, for the protection of staff, clearly set out whether it is appropriate for staff members to use personal digital cameras or mobile phones on field trips fro example and where such images are stored in school.

Acceptable Use of ICT Facilities within the School Library

A school library particularly in secondary schools can make the creation of a safe ICT learning environment more complex and challenging than in a formally designated teaching space.

A separate or additional acceptable use policy may be required for library use if there are any different technologies or services that pupils might have access to. For instance, some personal use by pupils may be acceptable.

Community Use

Where the school is used as a community resource, the use should be covered by an acceptable use agreement. This may be integral to the schools lettings policy. The management and monitoring may require extra technical work.

Areas of Teaching

Many links to Teaching and Learning resources are given through the website www.gowild.org.uk/esafety.

- **KS 1**

eSafety education should ideally be built into the curriculum from KS1. The fastest growing group of Internet users in the United States is 2-5 year olds (source: Behind the Screen, IPPR, 2008) and the nature of the Internet is such that once personal information is given away to contacts or websites online, there is no control over where that information will end up.

At KS1, children are beginning to become regular users of the Internet, not just from desktop computers but from mobile devices such as mobile phones and portable games consoles. At this age, eSafety education should focus on issues such as:

- Becoming aware of some of the benefits and risks of the Internet and other communication technologies, including how the Internet enables us to do many tasks in new or more efficient ways.
- Beginning to understand some of the qualities that can be used to assess if a person can be trusted, and to be aware of which adults in their lives they can safely turn to if they need help
- Identifying situations in which they should turn to a trusted adult for help
- Understanding that listening to their emotions can help them decide if a situation is unsafe
- Understanding what their personal information is, and that they should never give out their personal information online without asking a trusted adult first

- **KS 2**

Pupils at KS2 are beginning to use the Internet and other communications technologies with greater independence. The vast majority of pupils have access to an Internet-connected computer in a communal area at home such as the living room, but despite this 40% of 8-11 year olds say they use the computer mostly unsupervised. It's therefore important that they have a sound understanding of their personal information and how to keep this safe, as well as how to deal with inappropriate content and contact.

It is estimated that 70% of 11 year olds will own a mobile phone, thus safety training on using mobile phones needs to be in place in primary schools. This should cover personal safety issues such as using a mobile phone in public as well as being aware of the financial costs of using a mobile phone. Mobile technologies provide opportunities for cyberbullying to take place unnoticed and schools should address the issues of cyberbullying ensuring pupils do not dismiss it as 'just a bit of fun'.

Pupils are increasingly exposed to media content at this age, with 73% of 8-11 year olds having a television in their bedroom. Schools need to think about integrating media literacy into their eSafety provision so that pupils can begin to identify when and how they are being targeted for commercial purposes, how their personal information could be used for marketing and how to assess websites for reliability.

- **Secondary**

Young people see online technologies as an important vehicle for socialising with friends. They make constant use of instant messaging, mobile phone technologies and social networking sites to organise their social life. The Internet becomes more of a tool for research and communication rather than simply a fun distraction. (source: Byron Review, DCSF, 2008)

Young people increased independent exposure to media, spending an average of 25.5 hours a week consuming audio and visual media such as television, gaming consoles and online content. Young people spend between 3 and 4 hours a night interacting with instant messaging and social networking sites, with over half of all children having a profile. (source: Behind the Screen, IPPR, 2008)

Young people need to be empowered to take control of the technologies and Internet applications that they use, understanding the risks and benefits involved and being able to use them independently in a responsible and appropriate manner. Schools should ensure their eSafety provision makes specific reference to the common tools that young people use: instant messaging, peer-to-peer file-sharing, social networking sites, mobile phone technologies. Young people should also be taking control of their own hardware and software, ensuring they are protected from spyware, viruses, and trojans and that they are aware of the danger of spam and the possibilities for phishing and identity theft. They should be aware of how to keep hardware physically safe, especially when in public.

Responding to Incidents of Misuse

Even with all the policies and technological solutions in place, there may still be occasions when misuse of the internet and related technologies occur. Schools must ensure that they have appropriate strategies in place for responding to such instances.

Most incidents involve students and are minor in nature, but some are more serious and some may involve staff whose activity is inappropriate. An e-safety incident can cause uncertainty, through the nature of the incident or because of a lack of understanding of the potential seriousness.

- **Minor incidents**

These might be incidents of misuse by pupils such as copying information into assignments and failing to acknowledge the source (plagiarism and copyright infringement); downloading materials or images not relevant to their studies; misconduct associated with student logins, such as using some one else's password because they have forget there own.

Schools will have their own rules about particular technologies, and many of these issues will be covered within the school's acceptable use policy. In all but the most minor of cases it would be wise for the pupil to be issued with a warning, and the incident documented.

- **Incidents involving inappropriate materials or activities**

While not illegal, there will be some material that is just not appropriate within the school environment, and, in the case of staff, not in keeping with the professional standards or code of ethics of those who work with children and young people.

Incidents that involve inappropriate but legal material should be dealt with by the school via the usual disciplinary system; unless a criminal offence has been committed, it is not normally necessary to involve the police.

- **Incidents involving illegal materials or activities**

In the school context, very serious incidents tend to involve illegal materials (particularly the viewing, possession, making and distribution of indecent images of children) or serious stalking or harassment facilitated by communication technologies. Such criminal offences may be committed by staff and pupils alike. Discovery of indecent material within the school's network is a very serious situation, and must always be reported to the police. It is important that the material is not downloaded, printed or sent by email, because doing so will be an offence in itself. If at all possible, do absolutely nothing to the suspect computer or computers, including turning them on or off.

Staff, Governor and Visitor Acceptable Use Agreement

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is to help ensure that all staff are aware of their professional responsibilities when using any form of ICT and to help keep staff, governors and visitors safe. All staff are expected to sign this policy confirming their undertaking to adhere to its contents at all times. Any concerns or clarification should be discussed with <name of person in school>

- I will only use the school's email / Internet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number or personal email address, to pupils.
- I will only use the approved email system for any communications with pupils, parents and other school related activities.
- I will ensure that personal data (such as data held on the administration system) is kept secure and is used appropriately. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body and with appropriate levels of security in place.
- I will not install any hardware or software on school equipment without the permission of <name of person>
- I will report any accidental access to inappropriate materials immediately to my line manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with data protection policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher in line with data security policy.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to the Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. This includes ignoring invitations from pupils and parents to be part of their social networking site(s).
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this acceptable use policy and to support the safe use of ICT throughout the school

Signature Date

Full Name(printed)

Acceptable Use Agreement: Pupils - Primary

Form Group

Teacher

Pupil Acceptable Use Agreement

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use my own school email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my passwords for the Learning Platform, school network or for other learning websites.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT related contact with other children and adults is appropriate and polite.
- ✓ I will not deliberately look for, save or send anything that could offend others.
- ✓ If I accidentally find anything inappropriate on the internet I will tell my teacher immediately.
- ✓ I will not give out my personal details such as my name, phone number, home address or school.
- ✓ I will be responsible for my behaviour when using ICT in school or at home because I know that these rules are to keep me safe.
- ✓ I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ✓ I know that my use of ICT can be checked and that my parent or carer contacted if a member of school staff is concerned about my safety.

Signature Pupil.....

Signature Parent..... Date

Acceptable Use Agreement: Pupils – Secondary**Form Group****Teacher****Student Acceptable Use Agreement**

- I will only use ICT systems in school, including the internet, email, digital video or mobile technologies for school purposes.
- I will not download or install software on school equipment unless I have permission from a member of staff.
- I will only log on to the school network and Learning Platform (VLE) with my own user name and password.
- I will not reveal my passwords to anyone and change them regularly.
- I will ask my password to be reset if I forget it or suspect someone else knows it.
- I will only use my school email address for any activity related to school or in communicating with school staff.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will make sure that all ICT communications with other students, teachers and any other person is appropriate and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal.
- If I accidentally come across inappropriate material on the internet I will report it immediately to a member of staff.
- I will not give out any personal information such as name, phone number or address.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of students and/or staff will only be taken, stored and used for school purposes inline with school policy and not be distributed or shared outside the school network without the permission of the person(s) concerned.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others upset or bring the school into disrepute.
- I will respect the privacy and ownership of others' work on-line at all times.

- I will not attempt to bypass the internet filtering system through the use of proxy websites or any other means.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to teachers in school.
- I understand that this agreement is designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer will be contacted.

Signature Pupil.....

Signature Parent..... Date

eSafety Checklist for Schools

Description	Developing	In Place	Require Support
<ul style="list-style-type: none"> Does the school have an Acceptable Use Policy (AUP) for the use of its ICT systems? 			
<ul style="list-style-type: none"> Is the AUP regularly updated to take account of emerging technologies and events? 			
<ul style="list-style-type: none"> Do all stakeholders support the AUP: governors, senior management team, teaching staff, non-teaching staff, pupils and parents. 			
<ul style="list-style-type: none"> Has the school nominated a member of staff responsible for Internet safety and ensured they have received appropriate training. 			
<ul style="list-style-type: none"> Does the school provide information and engage parents regarding ICT use in school? 			
<ul style="list-style-type: none"> Have all pupils and parents/carers (where appropriate), read and signed the schools acceptable use agreement and had opportunity to ask questions about the agreement? 			
<ul style="list-style-type: none"> Have staff read and signed the schools acceptable use agreement and had opportunity to discuss the agreement. 			
<ul style="list-style-type: none"> Have students and staff been made aware of their individual responsibility to protect the security and confidentiality of the schools ICT systems? 			
<ul style="list-style-type: none"> Does the school provide appropriate opportunities to teach Internet safety to pupils and parents? Is there a scheme of work in place with progression through the Key Stages. 			
<ul style="list-style-type: none"> Do the school Anti-bullying and Behaviour Management policies make reference to electronic media and communication both inside and outside school? 			

<ul style="list-style-type: none"> Does the school Staff Handbook / Staff Code of Conduct refer to use of electronic media and communication both inside and outside school? 			
<ul style="list-style-type: none"> Are there procedures in place to deal with 'disclosure' by a child of a personal nature as a result of Internet safety education? 			
<ul style="list-style-type: none"> Has the school nominated a member of staff to be responsible for disclosure issues? 			
<ul style="list-style-type: none"> Is the school aware of how pupils' and staff use the Internet and email in school? 			
<ul style="list-style-type: none"> Have pupils and parents been advised that pupils' use of the Internet and e-mail systems may be monitored and what procedures and sanctions are in place should misuse occur? 			
<ul style="list-style-type: none"> Does the school adopt safe practices regarding the publication of the images and names of pupils and staff on its website? 			
<ul style="list-style-type: none"> Is the AUP supported by clearly defined procedures and appropriate sanctions should deliberate misuse or access to inappropriate materials occur? 			
<ul style="list-style-type: none"> Is the school aware of how to investigate allegations of misuse? 			
<ul style="list-style-type: none"> Are pupils and staff aware of the procedures for reporting accidental access to inappropriate materials on the Internet? 			

References and Resource Links

www.gowild.org.uk/esafety

From here you will find a weath of links to resources that will support the teaching of safety and Cyberbullying, many thanks to Kirklees Ednet for the initial work on identifying many relevant links.

Becta

Developing whole-school policies to support effective practice
<http://publications.becta.org.uk/display.cfm?resID=25934>

<http://www.becta.org.uk/schools/esafety>

<http://www.becta.org.uk/leaders/governors>

Yorkshire and Humberside Grid for Learning - YHGfL

<http://www.yhgfl.net/eSafety>

General

www.nen.gov.uk

National Education Network (NEN) - Guidance for Acceptable Use, The guidance has been developed by the NEN Safeguarding Group and supports the Becta ISP accreditation scheme, which itself is recommended by the Byron review (2008).

<http://www.kirklees-ednet.org.uk>

<http://www.Leedslearningnetwork.co.uk>

http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/

<http://www.tda.gov.uk/teachers/hottopics/esafety.aspx>

<http://www.digizen.org/cyberbullying/fullguidance/>

<http://www.nya.org.uk/information/111564/youthworkandsocialnetworking/>