E-safety Policy

Introduction

The school policy for E-safety was developed using the guidance provided from the E-safety Policy template produced by The South West Grid for Learning Trust (2013). It has been further developed by the Ambleside Primary Policy working group and agreed by the whole staff and has the full agreement of the Governing Body. The policy was approved and ratified by the Governing Body during the Autumn term 2014.

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Ambleside Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate E-safety behaviour that takes place out of school.

Aims

To ensure:

- responsible ICT use by all staff, pupils and the wider community; encouraged by education and made explicit through published policies.
- robust implementation of this e-safety policy in both administration and curriculum, including secure school network design and use.
- safe and secure Internet use including the effective management of filtering of inappropriate websites.
- staff, pupils and the wider community pupils have an awareness of how ICT, social media and the Internet is used in the world around them and its potential dangers.

Communication

When using communication technologies Ambleside Primary School considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to their line manager – in accordance with the school policy the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat, etc.) must be professional in tone and content.

- Phase leaders will determine whether whole class / group email addresses may be used or pupils provided with individual school email addresses for educational use.
- Pupils are taught about E-safety issues, such as the risks attached to the sharing of personal details. They are also **to** be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information is not posted on the school website and only official email addresses are used to identify members of staff.

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes all employees annually agree and sign a 'Statement of Acceptable Internet Use for Adults in School' (appendix 1) at the beginning of every academic year. This sets out clear guidance for staff to manage risk and behaviours online.

Ambleside Primary School has a duty of care to provide a safe learning environment for pupils and staff. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the academy through:
- limiting access to personal information
- training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk

School staff should ensure that:
- no reference is made in social media to pupils, parents / carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions are not to be attributed to the school /academy or local authority (LA)
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer to ensure compliance with the Data Protection Policies. Please refer to the Social Media Policy for further information.

Technical – infrastructure / equipment, filtering and monitoring

It is the responsibility of the academy to ensure that the managed service provider carries out all the E-safety measures that would otherwise be the responsibility of the academy, as suggested below. The managed service provider is fully aware of the school's E-safety and Acceptable Use of ICT Policies.

The school is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named within this policy will be effective in carrying out their E-safety responsibilities

School technical systems are always managed in ways that ensure that the school meets recommended technical requirements and refers to those outlined by the LA.

There are ongoing reviews and audits of the safety and security of school technical systems. Servers, wireless systems and cabling are securely located and physical access restricted. All users

have clearly defined access rights to school technical systems and devices at the appropriate level depending upon their position in school.

All users (as appropriate), are provided with a username and secure password. Staff users are responsible for the security of their username and password and are required to change their password every half term.

The administrator passwords for the school ICT system, are used and controlled by the ICT technician and are not shared unless by specific request of the head teacher.
Both the business manager and the ICT technician are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

Internet access is filtered for all users by the LA recommended network provider. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.

The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils). The ICT technician regularly monitors and records the activity of users on the school technical systems.

An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed. Please refer to Ambleside Primary School's Whistle Blowing Policy.

Appropriate and robust security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software, which is renewed annually.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet such as on social networking sites.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those

images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes such as mobile phones.

Care will always be taken when taking digital / video images that pupils are appropriately dressed and / or are not participating in activities that might bring the individuals or the school into disrepute. Pupils must not take, use, share, publish or distribute images of others without their permission. Photographs published on the website, or elsewhere that include pupils will be selected carefully will comply with good practice guidance on the use of such images and published only if the parent of the pupil has given permission for this on the school admission form. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the School's Data Protection Policy which adheres to the 1998 Act, which states that personal data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- kept no longer than is necessary
- processed in accordance with the data subject's rights
- secure
- only transferred to others with adequate protection.

Please refer to the Data Protection Policy for further information.

Staff must ensure that they:

- take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption and secure password protected devices

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below)**,** once it has been transferred or its use is complete

Role of Teaching and Support Staff

All teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of E-safety matters and of the current school E-safety policy and practices
- they have read, understood and signed the Statement of Acceptable Internet Use for Adults in School on an annual basis
- they report any suspected misuse or problem to the either head teacher or their line manager for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the E-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Education & Training Staff / Volunteers

It is essential that all staff receive E-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff should receive E-safety training as part of their induction programme, ensuring that they fully understand the school E-safety policy and Acceptable Use Agreements.
- The E-safety officer will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-safety policy and its updates will be presented to and discussed by staff in staff meetings
- The E-safety Officer or other nominated person such as a phase leader will provide advice / guidance / training to individuals as required.

Educating pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-safety is therefore an essential part of the school's E-safety provision. Children and young people need the help and support of the school to recognise and avoid E-safety risks and build their resilience.

E-safety is a focus in all areas of the curriculum and staff are all encouraged to reinforce E-safety messages across the curriculum whenever possible. The E-safety curriculum draws reference from E-safety materials from the internet, which have been purposefully planned and published for different ages to ensure they are broad, relevant and provide progression, with opportunities for creative activities.

The planning of the curriculum should also ensure that:

- Key E-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Pupils are taught in lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are helped to understand and encouraged to adopt safe and responsible use both within and outside school.
- Staff are expected to act as good role models in their use of digital technologies, the internet and mobile devices in lessons where internet use is pre-planned. Best practice ensures that pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the pupil's visit.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, this should be reported immediately to the police via the head teacher or E-safety officer.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible use, or very rarely, through deliberate misuse.
In the event of suspicion, all steps in the Whistle Blowing Policy should be adhered to.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. All incidents of misuse will be dealt with in line with the school's behaviour policy.

Role of the Governing Body

Governors are responsible for the approval of the E-safety Policy and for reviewing the effectiveness of the policy. This will be carried out by a member of the Governing Body who has taken on the role of *E-safety governor,* who also combines this role with that of the child protection / safeguarding governor). The role of the E-safety governor includes:

- meeting with the E-safety officer and ICT technician
- reporting to relevant governors' meetings

Role of the head teacher and other line managers

The head teacher has a duty of care for ensuring the safety (including E-safety) of members of the school community, though the day to day responsibility for E-safety will be delegated to the school deputies.

The head teacher, deputies and phase leaders are aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff.

The head teacher and other line managers at the school are responsible for ensuring that the E-safety Officer and other relevant staff receive suitable training to enable them to carry out their E-safety roles and to train other colleagues, as relevant.

Role of the E-safety officer

The deputy at the school who is responsible for health and safety will also take on the role of the E-safety lead officer. (Staff who have been trained as the designated safeguarding persons also combine this within their role if it is not a staff discipline matter which will be dealt with directly by the head teacher.)

The lead E-safety officer will:

- take on the day to day responsibility for E-safety issues and a role in establishing and reviewing the school E-safety policies / documents

- ensure that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place.
- provide training and advice for staff
- liaise with the LA / relevant body
- liaise with school technical staff
- receive reports of E-safety incidents and create a log of incidents to inform future E-safety developments if required
- meet with the E-safety governor and ICT technician to discuss current issues, review incident logs and filtering / change control logs
- reports when appropriate to the school leadership team

Role of Designated Safeguarding officer

To be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate online contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Although these are not technical issues, technology can provide a lead to child protection issues.

Role of the I.T. Technician

Although Ambleside Primary School has a managed ICT service provided by an outside contractor, it is still the responsibility of the school to ensure that the managed service provider carries out all the E-safety measures. The managed service provider is fully aware of the school E-safety policy and procedures.

The technical staff / co-ordinator for ICT / computing are responsible for ensuring that:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets required E-safety technical requirements and any local authority / other relevant body E-safety Policy / Guidance that may apply.
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- they keep up to date with E-safety technical information in order to effectively carry out their E-safety role and to inform and update others as relevant
- the use of the network / internet / remote access / email is regularly monitored in order that any misuse/ attempted misuse is reported immediately to the head teacher for investigation / action / sanction
- monitoring software / systems are implemented and updated as agreed in school policies

Role of the Parents/carers

Parents / carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local E-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good E-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / VLE and online student / pupil records
- their children's personal devices in the school (where this is allowed)

- advice on the school website which makes reference to the relevant web sites / publications such as www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Educating parents / carers

Many parents and carers may have only a limited understanding of E-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:
- curriculum activities
- letters, newsletters, web site
- parents / carers' evenings / sessions

Role of Pupils

All pupils are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy (Appendix 2)

It is important that they:
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- are expected to know and understand the use of mobile devices
- they hand in to the office any digital or mobile phone upon entering the premises and do not use it within school during the school day
- they should also know and understand the taking / use of images and on cyber-bullying
- understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the school's E-safety Policy covers their actions out of school, if related to their membership of the school

Racial & Equality Statement

All children have equal access and inclusive rights to the curriculum regardless of their age, gender, race, ethnicity, religion, belief, disability or ability. We plan work that is differentiated for the performance of all groups and individuals. Ambleside Primary School is committed to creating a positive climate that will enable everyone to work free from racial intimidation and harassment and to achieve their full potential. Policies are available on each of these that expand on this further.

All staff have equal access and inclusive rights to their work regardless of their age, gender, sexual orientation, race, ethnicity, religion, belief, disability or ability. Ambleside Primary School is committed to creating a positive climate that will enable everyone to work free from racial intimidation and harassment and to achieve their full potential. Policies are available on each of these that expand on this further.

Accessibility of policy documents

Parents and carers are welcome to ask for further information about any policy matter. Copies of all current School policies are available for parents and carers to read. A copy of each policy is displayed in the School lobby and all policies can also be consulted online via the School website at www.amblesideprimaryschool.co.uk. The School will try to arrange for the translation or summary of a document when this is requested by a parent or carer whose first language is not English.

Review

This policy will be reviewed in the Autumn term 2019.

Related Policies

Data Protection Policy
Whistle Blowing Policy
Social Media Policy
Safeguarding Policy
Anti-Bullying Policy
Child Protection Policy

Appendix 1

Statement of Acceptable Internet Use for Adults in School

The computer system is owned by Ambleside Primary School and is made available to staff to enhance their professional activities including teaching, learning, communications, research, administration and management. The school's acceptable use policy has been drawn up to protect all parties to include adults and the school

The following points are considered acceptable use on school premises:

- All internet use should be appropriate to staff professional conduct activities.
- Sites and materials accessed must be appropriate to work in school. All users that recognise and use materials that are inappropriate should expect to have their access removed with immediate effect.
- Access should only be used via authorised username and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT systems, or that attacks and corrupts other systems is forbidden.
- Users are responsible for all email sent and for contacts made that may result in email being received.
- The same professional levels of language and content should be applied as for letters or other media, particularly as emails are often forwarded.
- Posting anonymous messages or forwarding chain letters is forbidden.
- Personal shopping and browsing for personal shopping, including e-bay is forbidden at school.
- Use for financial gain, gambling, political purposes or advertising is forbidden at school.
- Use for downloading films, music and TV for personal use is forbidden at school.

Guidance for safeguarding staff as employees of Ambleside Primary School:
It is advisable that staff should:

- Not publish photographs of school pupils in any form on their personal web pages, facebook, blog or own site.
- Not name the school on their personal web pages, blog or site.
- Ask colleagues' permission before publishing photos of them on their web pages, blog or site.
- Remain professional in any comments made on the internet regarding any aspect of school life.
- Not enable parents or pupils to access photos that could be considered compromising through social network sites such as Facebook and My Space.

The school will not be liable for any damages incurred by or relating to abuse of this policy.
I have read the acceptable internet usage statement and agree to uphold these statements.

Signed: Date:

Appendix 2

Internet Safety Rules

- On the internet I will only use my own login username and password.
- I will not look at, change or delete other people's work/files.
- I will ask permission before entering any website, unless my teacher has already approved that site.
- I will only send email my teacher has approved. I will make sure the messages I send are polite and sensible.
- When sending email I will not send my full name, address, phone number or arrange to meet anyone.
- I understand that I am not allowed to enter internet chat rooms whilst using school computers.
- If I see anything I am unhappy with or receive messages I do not like, I will tell a teacher immediately.

I understand that if I deliberately break these rules I will be stopped from using the internet and will receive appropriate sanctions following the school behaviour policy.

Pupil's signature

Date

ACHIEVE BE PROUD SUCCEED Together

Appendix 3

Ambleside Primary School
Minver Crescent
Aspley
Nottingham
NG8 5PN

Telephone: (0115) 900 3610
Fax: (0115) 900 3620
Email:
admin@ambleside.nottingham.sch.uk
www.amblesideprimaryschool.co.uk
Head Teacher – Mrs Karen L. Hannon

Dear Parents & Carers,

Use of the Internet

Thank you for all the positive feedback we have received concerning our school website (www.amblesideprimaryschool.co.uk) and 'Mathletics' which many of the children are enjoying using regularly at home.

As Part of your child's curriculum and the development of ICT skills, Ambleside Primary School is providing supervised access to the internet. We believe that the use of the internet is worthwhile and is an essential skill as they grow up in the modern world today. Please read the attached rules for responsible internet use and discuss them with your child.

Although there are certain risks associated with internet use we have taken steps to ensure these are kept to an absolute minimum. Our School Internet provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home, but your internet provider may be able to offer a 'nanny filter' which will let you restrict your child's access to inappropriate sites.

At Ambleside Primary School, we take the following steps to ensure acceptable use of the internet:

- Use of a filtered Internet Service Provider
- Children's use of the internet is a supervised activity
- Websites used by the children will be viewed by staff prior to use and also regular checks will be made on the computer's Internet browser, bookmarks, cache or history.
- Children will be informed about and understand the attached Rules for Responsible Internet Use

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through inappropriate Internet use. As long as your child follows rules and instructions their use of the internet should be safe and appropriate.

If you have any concerns please do not hesitate to contact the school for further information.
Yours sincerely,

Karen Hannon
Head Teacher

Appendix 4

Activities	Key E-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved online materials.	Web directories e.g. Ikeep bookmarks Webquest UK
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids Yahooligans CBBC Search Kidsclick Google
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. Super Clubs.	RM Easy Mail Super Clubs PLUS Gold Star Café School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	Making the News Super Clubs Info mapper Headline History Kent Grid for Learning Focus on Film
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News Super Clubs Learning grids Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	Super Clubs Skype Flash Meeting
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype Flash Meeting National Archives "On-Line" Global Leap Natural History Museum Imperial War Museum