Air Balloon Hill PRIMARY School

E-Safety

and

Social Media Policy

(Including Home and Acceptable use)

Ratified by the Governing Body	**6/02/2016**
Review Cycle	**Annual**
Review Date	**6/02/2018**

Date adopted: 13th October 2014

History of most recent policy reviews	**Date of amendments**	**By**
Original E-Safety and ICT Acceptable Use Policies combined and re-written September 2014	September 2014	Full Governing Body
Review of E-safety Policy	November 2016	E-safety Committee
Combination of E-Safety and Social Media Policy	November 2016	E-Safety Committee
Ratified FGB	February 2017	Full Governing Body

Contents

Development / Monitoring / Review of this Policy

This e-safety policy has been adapted from a template produced by SWGfL and customised by a working group made up of:

- Headteacher
- IT Manager
- E-Safety Co-ordinator
- E-Safety Governor
- Communications Governor

Air Balloon Hill Primary is committed to safeguarding and promoting the welfare of children
and expects all staff and volunteers to share this commitment.

Aims

To set out the key principles and code of conduct expected of all members of staff, governors, Friends and volunteers at Air Balloon Hill Primary School with respect to social networking.

To further safeguard and protect children and staff.

Objectives

E-Safety

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 Headteachers to such extent as is reasonable, to regulate the behaviour of students / 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.

Air Balloon Hill 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 take place out of school.

Social Media

This policy sets out Air Balloon Hill Primary School policy on social networking. Social networking activities conducted online outside work, such as blogging, involvement in social networking sites such as Facebook or Twitter and posting material, images or comments on sites such as You Tube can have a negative effect on an organisation's reputation or image.

In addition, Air Balloon Hill Primary School has a firm commitment to safeguarding children in all aspects of its work. This policy has been written to set out the key principles and code of conduct that we expect of all members of staff with respect to their responsibilities in connection with the use of social networking sites.

Key Principles

Everyone at Air Balloon Hill Primary School has a responsibility to ensure that they protect the reputation of the school, and to treat colleagues and members of the school with professionalism and respect.

- It is important to protect everyone at Air Balloon Hill Primary School from allegations and misinterpretations which can arise from the use of social networking sites.
- Safeguarding children is a key responsibility of all members of staff and it is essential that everyone at Air Balloon Hill Primary School considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the school either as a paid employee or volunteer must not communicate with **pupils past or present under 18**. The only exception to this is their own children; any pupils who are their children's friends should not be communicated with through social media.
- This policy relates to social networking outside work. Blogging and accessing social networking sites at work or at home using school equipment is not permitted, unless for professional purposes and authorised by the Headteacher. Personal mobile phones **should only be used in non-contact time with children.**

Scope of the Policy

Roles and Responsibilities

All the staff at Air Balloon Hill Primary School share responsibility for the E-Safety Policy. The school will ensure that IT lessons, assemblies, PSHE lessons, and an age-appropriate curriculum for e-safety will support pupils to become safe and responsible users of new technologies. The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governors

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 the Finance Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Link Governor.

The role of the E-Safety Link Governor will include:

- regular meetings with the E-Safety Co-ordinator or Deputy Child Protection Officer
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meetings

Headteacher and Senior Leadership Team

- The Headteacher 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 E-Safety Co-ordinator.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (**Appendix A** - Responding to Incidents of Misuse)
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher keeps the e-safety incident logs and ensures that staff are trained on how to report incidents.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

E-Safety Coordinator

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents

- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

- provides training and advice for staff

- liaises with the Local Authority

- liaises with school technical staff

- receives reports of e-safety incidents (Appendix J Record of reviewing devices / internet sites) and creates a log of incidents to inform future e-safety developments, (Appendix B - Log Sheet for E-Safety Incidents).

- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering

- attends relevant committee meetings of Governors

IT Manager

The IT Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack

- that the school meets required E-safety technical requirements and any Local Authority E-Safety Policy or Guidance that may apply.

- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

- that 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

- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher / Senior Leader; E-Safety Coordinator investigation, action or sanction

- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

All staff at Air Balloon Hill Primary School 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 Home School Agreement & Pupil Acceptable Use Agreement (KS2) (**Appendix C**) or Home School Agreement & Pupil Acceptable Use Agreement (Foundation / KS1) (**Appendix D**)

- they report any suspected misuse or problem to the Headteacher, a Senior Leader or E-Safety Coordinator for investigation, action or sanction

- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school email

- 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 (e.g. the appropriate use of cameras on school trips/projects)

- 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

Designated Child Protection Officer and Deputy DCPO

Both the Designated Child Protection and Deputy DCP Officers at Air Balloon Hill Primary School should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

NB. These are child protection issues, not technical issues, it is simply that the technology provides additional means for child protection issues to develop.

E-Safety Committee

The E-Safety Committee provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body and the production of an annual report to Governors.

Members of the E-Safety Committee will assist the E-Safety Coordinator with:

- the production, review and monitoring of the school e-safety policy and documents.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the pupils about the e-safety provision

Pupils

All pupils at Air Balloon Hill Primary School are responsible for using the school digital technology systems in accordance with the Home School Agreement & Pupil Acceptable Use Agreement (KS2) (**Appendix C**) or Home School Agreement & Pupil Acceptable Use Agreement (Foundation / KS1) (**Appendix D**)

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should 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

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, and the school website.

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
- Social Media websites, in particular, ensuring that no images of children taken on the school premises or whilst on school trips or events are uploaded onto any social media sites (including Facebook and YouTube)

Policy Statements

Education – pupils

Air Balloon Hill Primary School recognises that the educational benefits of internet access far outweigh the possible risks and good planning and management will ensure appropriate and effective pupil use.

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach and this forms an essential part of the school's E-Safety and Social Media Policy. 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 should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities that enhance childrens' awareness and understanding.

Authorisation for Internet Access

Pupils' will be asked to sign the ICT Acceptable Use Policy Agreement at the beginning of Reception (**Appendix D**); at the start of Year 3 (**Appendix C**) or when a new pupil starts at the school. Parents/carers are also asked to sign a permission slip and Home User Agreement (**Appendix E**) for their child/ren which should be returned to school office. A log of the permission slip will be kept in the School Office.

Internet access will be granted to a whole class or individuals as part of a scheme of work, after suitable education in responsible internet use. Older pupils may carry out their own internet searches for research purposes and should know how to conduct searches safely and what to do if they come across something unsuitable.

Pupils' entitlement to use the internet is based on their responsible use of it. Irresponsible use may result in this privilege being removed.

Education - Parents / Carers

Many parents and carers 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 on-line 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 evenings
- High profile events e.g. Safer Internet Day

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. (**Appendix H**)
- The E-Safety Coordinator (or another nominated person) 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 prior to Governor review.
- Training Audits are managed by the Business Manager.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / Bristol City Council Governor Development Service / or other relevant organisation (eg SWGfL).
- Participation in school based training / information session

Social Media and Mobile Phones - Protecting Professional Identity

All adults working with children have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of children. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, children, and public in general those with whom they work with. Adults in contact with children should therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.

The guidance contained in this policy is an attempt to identify what behaviours are expected of schools' staff who work with children. Anyone whose practice deviates from this document and/or their professional or employment-related code of conduct may bring into question their suitability to work with children and young people and may result in disciplinary action being taken against them.

School staff should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential to the designated safeguarding lead and will be recorded on CPOMS.

Code of Conduct: Social Networking

Under no circumstances should staff make reference to any staff member, pupil, parent or school activity/event.

The following are also **not considered acceptable** at Air Balloon Hill Primary School:

- The use of the school's name, logo, or any other published material without written prior permission from the Headteacher. This applies to any published material including the internet or written documentation.

- The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.

- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.

- The posting of any images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities.

- The acceptance of friend requests from pupils past or present **under 18 years** of age. It is also unwise to accept friend requests from parents or carers of pupils past or present from Air Balloon Hill Primary School.

Be aware that your reputation could be harmed by what others share about you online, such as friends tagging you in inappropriate posts, photographs or videos.

In addition to the above everyone at Air Balloon Hill Primary School must ensure that they:

- Communicate with children and parents in an open and transparent way using the school phone number and email address.

- Never 'friend' a pupil at the school past or present and under 18 years of age.

- Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school.

- Use social networking sites responsibly and ensure that neither their personal nor professional reputation, nor the school's reputation is compromised by inappropriate postings.

- Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.

Potential and Actual Breaches of the Code of Conduct

In instances where there has been a breach of the above Code of Conduct, the following will apply:

- Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Disciplinary Procedure. A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school's ethos and principles.
- The Governing Body will take appropriate action in order to protect the school's reputation and that of its staff, parents, governors, children and anyone else directly linked to the school.

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff will always advise the Headteacher of the justification for any such action already taken or proposed.

The Headteacher will in turn seek advice from Bristol City Council where appropriate and may refer to external organisations for guidance. This policy takes account of employment legislation and best practice guidelines in relation to social networking in addition to the legal obligations of governing bodies and the relevant legislation.

Safer Online Behaviour

Some social networking sites and other web-based sites have fields in the user profile for job title etc.

If you are an employee of a school and particularly if you are a teacher, you should not put any information onto the site that could identify either your profession or the school where you work. In some circumstances this could damage the reputation of the school, the profession or the local authority.

In their own interests, staff need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers.

This will avoid the potential for children or their families or friends having access to staff outside of the school environment.

It also reduces the potential for identity theft by third parties. All staff, particularly new staff, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate.

This includes any photographs that may cause embarrassment to themselves and the school if they are published outside of the site.

Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character.

Making allegations on social networking sites (even in their own time and in their own homes) about other employees, children or other individuals connected with the school, or another school, or Bristol City Council could result in formal action being taken against them.

This includes the uploading of photographs which might put the school into disrepute.

Technical – infrastructure / equipment, filtering and monitoring

Air Balloon Hill Primary School will be 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.

Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so; because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the Local Authority. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists.

Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the IT Manager.

In the event of the IT Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher

Mobile devices that access the school internet connection (whether school / academy or personal devices) will be subject to the same filtering standards as other devices on the school systems

Any filtering issues should be reported immediately to the IT Manager who will notify the filtering provider.

Requests from staff for sites to be removed from the filtered list will be considered by the IT Manager and Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.

Publishing on the internet

The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

- The point of contact on the school website should be the school address, school e-mail and telephone number. Staff or pupils' home information will NOT be published.

- Photographs used on the website will not identity individual pupils. Group shots or pictures taken over shoulders will be used where possible and other carefully selected shots at the discretion of the Headteacher.

- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

- Parents are invited to notify the school if they do not wish their child's photograph to be published on the school website. Parents will be notified of their right to refuse to allow any pictures of their child to be shown. Parents are notified of this right annually in the Autumn Term or when their child starts school.

- Where audio and video are included, the nature of the items uploaded will not include content that allows the pupils to be identified.

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.

Mobile Phones / Cameras / Video Recorder Usage

To ensure the safety and welfare of children in our care personal mobile phones, cameras and video recorders must not be used when children are present.

- Personal mobile phones should only be used on the school premises when in non-contact time with children and only used during work time in exceptional circumstances, which have been discussed and agreed with a member of the leadership team.
- Photographs or images of any children within our care may only be taken following parental consent and only using one of the school cameras / iPads. These images should remain within this setting or be shared only with the parents of the child concerned.
- Personal mobiles, cameras or video recorders cannot be used to record classroom activities. ONLY school property can be used for this.
- School photographs and recordings can only be transferred to and stored on a school computer.
- All personal mobile phones must be kept in a secure place (not in a pocket), switched off and not be accessed throughout contact time with the children.
- In exceptional circumstances, which have been discussed and agreed with a member of the leadership team, staff may keep their phone switched on and accessible as long as they use their phone out of view of children, i.e. in a room designated for staff, e.g. the staff room or an office.
- During school visits mobile phones should be used away from the children and for emergency purposes only.

Data Protection

Protection of Personal Information

Staff should not give their personal e-mail addresses to children or parents. Where there is a need for communication to be sent electronically the school e-mail address should be used. Likewise staff should keep their personal phone numbers private and not use their own mobile phones to contact children or parents in a professional capacity.

There will be occasions when there are social contacts between children and staff, where for example the parent and teacher are part of the same social circle or staff are transport escorts.

These contacts however, will be easily recognised and openly acknowledged. Staff have a responsibility to make any such contact known to the senior leadership team.

Staff should never share their work log-ins or passwords with other people.

Staff are advised to understand who is allowed to view the content on their pages of the sites they use and how to restrict access to certain groups of people.

Access to Inappropriate Images and Internet Usage

There are no circumstances that will justify adults possessing indecent images of children. Staff who access and possess links to such websites will be viewed as a significant and potential threat to children

.

Accessing, making and storing indecent images of children are illegal. This will lead to criminal investigation and the individual being barred from working with children, if proven.

Staff should not use equipment belonging to their school/service to access any pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

Where indecent images of children are found by staff, the police should be immediately informed. Schools should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

Where other unsuitable material is found, which may not be illegal but which raises concerns about that member of staff, Bristol City Council should be informed and advice sought. The school should not attempt to investigate or evaluate the material themselves until such advice is received.

Full details can be found in the school's Data Protection Policy. A copy is available on the school website or from the school office.

Cyberbullying

Air Balloon Hill Primary School definition of cyberbullying is 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual and/or to attempt to gain power and control over them.'

In order to reduce the potential for cyberbullying children are not allowed to bring phones to school. Only Y6 children who walk to school alone are permitted to bring mobile phones to school.

In this circumstance, mobile phones will be handed to the teacher and locked away during the school day.

Prevention activities are key to ensuring that staff are protected from the potential threat of cyberbullying.

All employees are reminded of the need to protect themselves from the potential threat of cyberbullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.

If cyberbullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails.

Staff are encouraged to report all incidents of cyberbullying to their line manager or the Headteacher. Permission to take screen prints of messages or web pages should be sought and a careful log of the time, date and place of the site should be created.

All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident.
It is for the individual who is being bullied to decide whether they wish to report the actions to the police.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other Adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X						X	
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X							X
Taking photos on personal mobile phones / cameras				X				X
Taking photos on school cameras	X						X	
Use of other mobile devices eg tablets, gaming devices		X	X					X
Use of personal email addresses in school, or on school network	X							X
Use of school email for personal emails				X				X
Use of messaging apps				X				X
Use of social media				X				X
Use of blogs		X				X		

When using communication technologies the 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 the designated safeguarding lead – 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 students / pupils or parents / carers (email, chat, etc) must be professional in tone and content. Communications between staff and parents/carers/pupils may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

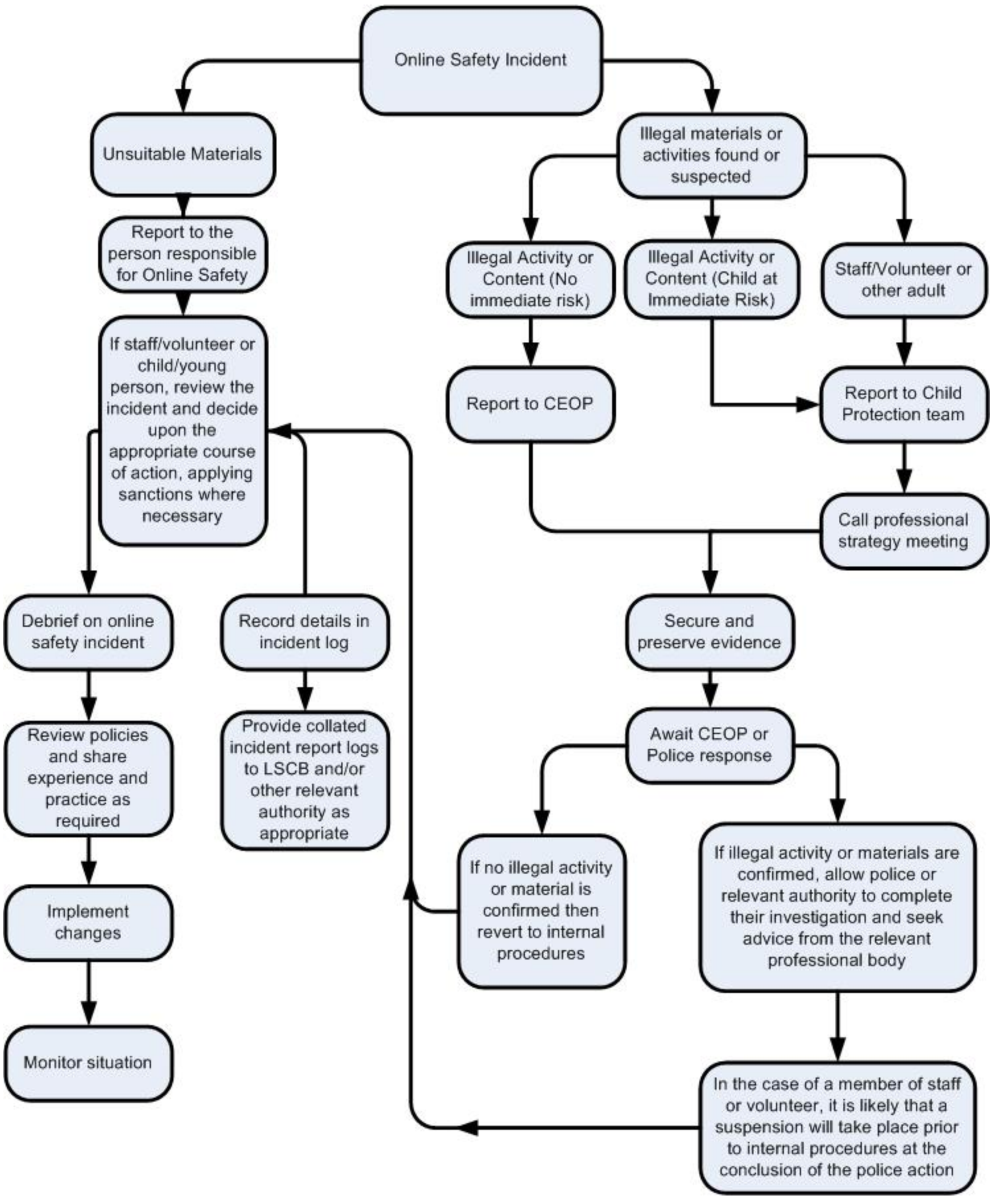
		Staff & other Adults					Pupils				
User Actions		Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Not allowed and illegal	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed	Not allowed and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X					X
	pornography				X					X	
	promotion of any kind of discrimination				X					X	
	threatening behaviour, including promotion of physical violence or mental harm				X					X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X					X	
Using school systems to run a private business					X					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X					X	
Infringing copyright					X					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X					X	
Creating or propagating computer viruses or other harmful files					X					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X					X	
On-line gaming (educational)		X							X		
On-line gaming (non educational)					X					X	
On-line gambling					X					X	
On-line shopping / commerce			X							X	
Use of social media			X							X	
Use of messaging apps			X							X	
Use of video broadcasting eg Youtube				X						X	

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. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

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, refer to the right hand side of the Flowchart (below and Appendices A and L) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

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 or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation. It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

The completed form should be retained by the Headteacher for evidence and reference purposes.

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. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Pupils

Incidents:	Refer to class teacher	Refer to Deputy Headteacher **	Refer to Headteacher **	Refer to Police	Refer to IT Manager for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			
Unauthorised use of non-educational sites during lessons	X				X		
Unauthorised use of mobile phone / digital camera / other mobile device	X	X					
Unauthorised use of social media / messaging apps / personal email	X	X					
Unauthorised downloading or uploading of files	X				X		
Allowing others to access school network by sharing username and passwords	X				X		
Attempting to access or accessing the school network, using another pupil's account		X			X		
Attempting to access or accessing the school network, using the account of a member of staff		X	X		X		
Corrupting or destroying the data of other users		X			X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X	
Continued infringements of the above, following previous warnings or sanctions			X	X		X	
Actions which could bring the school into disrepute or breach the		X	X			X	

integrity of the ethos of the school							
Using proxy sites or other means to subvert the school's / academy's filtering system		X			X		
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X		
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X		X		

** Referrals to the Deputy Headteacher or Headteacher will then follow the School Behaviour Policy for appropriate sanctions

Staff

Incidents:	Refer to Line Manager	Refer to Headteacher **	Refer to Local Authority / HR **	Refer to Police	Refer to IT Manager for action re filtering etc
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	
Inappropriate personal use of the internet / social media / personal email	X	X			X
Unauthorised downloading or uploading of files	X	X			X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X			X
Careless use of personal data eg holding or transferring data in an insecure manner	X	X			X
Deliberate actions to breach data protection or network security rules	X	X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X	X	
Actions which could compromise the staff member's professional standing	X	X	X		
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	X	X	X		
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	

Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X
Breaching copyright or licensing regulations	X	X			
Continued infringements of the above, following previous warnings or sanctions	X	X	X		

** Referrals to the Headteacher or HR/LA will then follow the School Disciplinary Policy for appropriate sanctions

Linked Policies

This E-Safety Policy and the appendices should be read in conjunction with other related School Policies:

- Child Protection Policy
- Anti-Bullying Policy
- School Behaviour Policy
- Data Protection Policy
- Freedom of Information Policy
- Confidentiality Policy
- Code of Conduct for School Employees
- Code of Practice on the Conduct of Investigations
- Model Disciplinary Policy

Complaints

Responsibility for handling incidents will be given to the Headteacher or delegated as the need arises.

Any complaint about staff misuse must be referred to the Headteacher and then to Chair of Governors following the school's Complaint Policy.

Any illegal apparent or actual misuse will be reported to the Headteacher or the police, as appropriate. (**Appendix A**)

Complaints about misuse of the internet in school by pupils must follow the most relevant schools policy (i.e. Behaviour, Anti-Bullying)

Legislation

There is a variety of legislation under which this E-Safety Policy has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

Air Balloon Hill Primary School will consider legal advice in the advent of an e safety issue or situation:

Computer Misuse Act 1990
Data Protection Act 1998
Freedom of Information Act 2000
Malicious Communications Act 1988
Regulation of Investigatory Powers Act 2000

Trade Marks Act 1994
Copyright, Designs and Patents Act 1988
Telecommunications Act 1984
Criminal Justice & Public Order Act 1994
Racial and Religious Hatred Act 2006
Protection from Harassment Act 1997
Protection of Children Act 1978
Sexual Offences Act 2003
Public Order Act 1986 (This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written)
Obscene Publications Act 1959 and 1964
Human Rights Act 1998
The Education and Inspections Act 2006
The Education and Inspections Act 2011
The School Information Regulations 2012

Acknowledgements

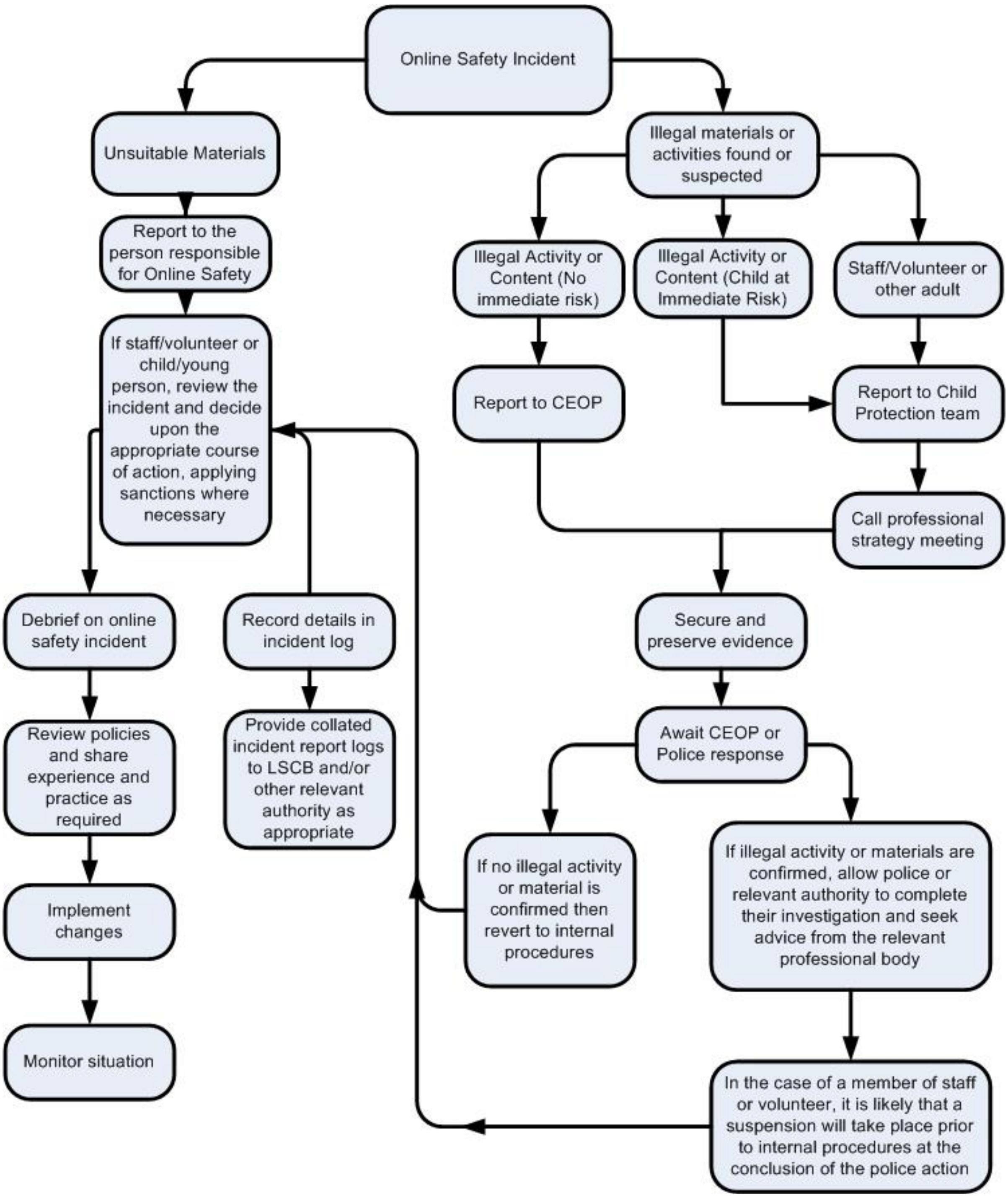
This Policy has been adapted from a template produced by SWGfL which was drawn up in conjunction with a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this E-Safety Policy:

- Members of the SWGfL E-Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Appendices

Can be found on the following pages:

APPENDIX A - Responding to incidents of misuse – flow chart


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

APPENDIX B - Reporting Log

ABHPS ICT Incident Reporting Form				**Agreed actions taken**	
Date of Incident:	Time of Incident	ICT Incident Reported By	Incident details, including names of any pupils/staff involved	What?	By Whom?
Date Reported	Time Reported	Incident Reported to		Review Date	Signature
Comments:					

APPENDIX C – Home School Agreement & Pupil Acceptable Use Agreement (KS2)

At Air Balloon Hill Primary School, we believe that pupils have the right to safe internet access at all times. The internet is a powerful tool, which opens up new opportunities for everyone. This Acceptable Use Agreement is designed to increase your awareness of e-safety and help you to use the school technologies responsibly and safely to enhance your learning.

- I understand that I must use school ICT systems in a responsible way, to ensure that I stay safe and there is no risk to the safety and security of the ICT systems and other users.

- I understand that the school will monitor my use of the systems, devices and digital communications.

- I will be aware of "stranger danger", when I am communicating on-line.

- I will NEVER tell anyone I meet on the internet any personal information about myself or others; this includes my home address, my telephone number or my school's name without permission, or send a picture of myself. I will NEVER arrange to meet anyone in person.

- If I see anything online which makes me feel uncomfortable, upset or worried, I will tell a trusted adult immediately.

- I will never answer unpleasant, suggestive or bullying emails or messages and I will always report them to a trusted adult. I know not to delete them straight away but show them to the person I have reported it to, as evidence.

- I will always be myself and not pretend to be anyone or anything I am not. I know that the posting of anonymous messages and the forwarding of chain messages is not allowed.

- I understand that I will only be allowed to use the internet if I use it responsibly and if I do not, I may not be allowed to use the internet at school.

- I know that being responsible means I should not look for bad language, inappropriate images or violent games, and I know that if I accidentally come across any I should report it to a teacher or parent/carer. I know that my teacher can check the websites I have visited.

- I will treat my password like my toothbrush –and not share it with anyone (even my best friend), and I will log off when I have finished using the computer.

- I will be polite and sensible when I email others and not send, or encourage, material which may offend or annoy others or invade another person's privacy. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.

- I know that I am not allowed on personal e-mail, social networking sites or instant messaging in school.

- I know that if I walk to or from school unaccompanied by my parent/carer, I may bring a mobile phone into school. I understand that this must be handed into my class teacher, school office or the Headteacher first thing in the morning to be locked away. I understand that my phone remains my responsibility and is left at my own risk.

- I will not take or distribute images of anyone without their permission.

When using the internet for research or recreation, I agree that:

- At school, I will not download any software from the internet.
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not use social media sites at any time whilst in school or using school equipment.
- If I accidently discover anything on the internet that is inappropriate or I feel uncomfortable about, I will report it to my teacher or member of staff in the IT suite immediately.
- Information on the internet may not always be reliable and I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me. I know that some websites may be sponsored by advertisers.
- I will ensure that I have permission to use the original work of others in my own work and where work is protected by copyright, I will not try to download copies (including music and videos)

I understand that I am responsible for my actions, both in and out of school

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to sanctions as outlined in the School Behaviour Policy. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents/carers and in the event of illegal activities involvement of the police.

I have read and understand the above and agree to follow the School's ICT Acceptable Use Policy guidelines:

Name of Pupil: Class:

Signed: Date:

Parent / Carer Countersignature
I have discussed the above points with my child and agree to them being allowed to used the computers and internet whilst at school

Parent / Carers Name:

Signed: Date:

Parents/carers are also asked to complete the Parent/Carer Acceptable Use Form (Appendix E)

APPENDIX D - Pupil Acceptable Use Agreement (Foundation / KS1)

At Air Balloon Hill Primary School, we believe that pupils have the right to safe internet access at all times.

We ask parents of children in Foundation Stage and Key Stage 1 to discuss the points below with their child regarding e-safety.

This is how we stay safe when we use computers:

- Children must ask a teacher or trusted adult if they want to use the computers
- Children will only use activities that a teacher or suitable adult has told or allowed them to use.
- Children will take care of the computer and other equipment
- Children will ask for help from a teacher or suitable adult if they are not sure what to do or if they think they have done something wrong.
- Children will tell a teacher or trusted adult if they see something that upsets them on the screen.
- Children know that if they break the rules they might not be allowed to use a computer.

Name of Pupil:

Class:

Date:

Parent / Carer Countersignature

I have discussed the above points with my child and agree to them being allowed to used the computers and internet whilst at school

Parent / Carers Name:

Signed: Date:

Parents/carers are also asked to complete the Parent/Carer Acceptable Use Form (**Appendix E**)

APPENDIX E - Parent/Carer Acceptable Use Agreement

The internet and digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

Unfortunately, the use of the internet is not without its dangers and some materials accessible through it are inappropriate for primary school aged children. However, whereas no system can be guaranteed to be 100% safe, the huge benefits far outweigh the disadvantages and every reasonable precaution, including monitoring and filtering systems, are used to ensure that children will be safe when they use the internet and ICT systems.

Whilst the school monitors ICT use in school it needs to be understood that children also have an important responsibility themselves as to how they use the internet and school equipment. Please read through the E-Safety Policy and ICT Acceptable Use Policy Agreement with your child; discuss the points with them and impress upon them how important they are.

This Acceptable Use Policy is intended to ensure that:

- young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. Parents/carers are requested to sign the permission form below to show their support of the school in this important aspect of the school’s work.

Photographs/Video Images

Air Balloon Hill Primary School respectfully requests that Parents/carers refrain from using mobile phones in the playground so that their motives cannot be misinterpreted due to the sensitivities regarding the photographing of children. However, we recognise that there are many circumstances where a parent or carer will wish to take photographs or video images of their child at school events.

In order to comply with the Data Protection Act we invite parents/carers to inform us if they do not wish their child to be filmed or photographed by filling in the slip on (**Appendix F**) and returning it to the school office. If we do not receive a signed form, we will assume that you are happy for your child to be filmed or photographed under the circumstances which the school feels are appropriate and for photographs to be posted on our website; used in displays; or reproduced in printed materials authorised by the school.

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:

- **Images taken on the school grounds <u>must not</u> be published/made publicly available on social networking sites (for example Facebook),**

- Parents/carers **<u>must not</u>** comment on any activities involving other pupils in the digital / video images.

- We would expect other parents to report anything that they see on social media sites or online that they are unhappy about, including photographs of children at the school or other material which is detrimental to the school or individual children. This should be reported to the Headteacher and we may, in turn, report the matter to the Police.

It is expected that parents/carers taking photographs or video images at school events will abide by the above guidelines. Any parent/carer found to be uploading images taken at school events or sharing those images with others will be asked to take down the images and may be requested to meet with the Headteacher and Chair of Governors and/or may be banned from any future school events or from the school site.

Declaration and Permission Form

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

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

I have read and discussed the E-Safety Policy and ICT Acceptable Use Policy Agreement with my child and agree to support the school's E-Safety policy.

I have read the above information about the taking of photographs/video images at school events and I agree to abide by the guidelines. I understand that any breach of these guidelines may result in me being banned from attending future school events.

As the parent / carer of the above pupil, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

For pupils in KS2 (Years 3-6)

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet - both in and out of school.

For pupils in Foundation Stage and KS1 (Reception & Years 1-2)

I have discussed the Acceptable Use Agreement with my son / daughter and will them to understand the importance of safe use of technology and the internet - both in and out of school.

Parent / Carers Name: Pupil Name:

Signed: Date:

Name of first parent/carer

Signed: Date:

Name of second parent/carer

APPENDIX F - Photographs and the Use of Digital / Video Images

During the course of their school life, there will be lots of events in school at which parents/carers will want to take photographs or record video images of their children performing.

In addition, we may also be approached by members of the media wanting to take pictures or record film footage of our pupils in connection with activities such as productions, concerts, or other activities taking place at the school.

Publicity can be of great benefit in the wider recognition it offers for the achievements of children at the school. We would therefore like to be able to offer the media the chance to take pictures and film where this is appropriate.

Finally, there may be occasions when we would like to take and display photographs of children at the school and on our website, again, in order to promote the school and the achievements of pupils in an appropriate way.

These photographs may also be used in school brochures or other printed materials authorised by the school.

We recognise that there may be circumstances where a parent or carer will not wish their child to be filmed or photographed. We are therefore inviting you to let us know if this is the case by filling in the slip below and returning it to the school. If you tick ‘No’, your child will be removed from the activity taking place, so that other parents /carers may continue to take photographs.

It is intended that the preferences you indicate on this slip will remain in place throughout your child’s time at Air Balloon Hill Primary School and we ask that if these preferences change at any time, you notify the school immediately.

Any photographs or video images taken on the school site or as part of a school-led activity (e.g. a school trip) are done so in good faith and therefore must NOT under any circumstances be posted on or uploaded to the internet and, in particular, to social media or networking sites such as Facebook.

Please read the statements below and tick either Yes or No to indicate your consent. If we do not hear from you, we will assume that you are happy for your child to be filmed or photographed under circumstances which the school feels are appropriate and for photographs to be posted on our website, used in displays, or reproduced in printed materials authorised by the school.

If you have any concerns or wish to discuss this further please contact the headteacher.

Reply Slip - Photographs and Video Images

		Yes	No
A	I agree to my child’s picture / photograph being used on the school website.	□	□
B	I agree to my child appearing on TV, or being included in radio programmes in connection with the school	□	□
C	I agree to my child appearing on TV, or being included in radio programmes in connection with the school	□	□
D	I agree that my child may participate in events at school, at which photographs and video images are being taken by other parents/carers (including, but not limited to, the Nativity Play; Class Assemblies and Sports Days)	□	□
E	I agree that photographs and video footage that I have taken during school events will NOT be uploaded to the internet or posted on any social media or networking sites - including Facebook	□	

Signed: ______________________________ **Date:** ____________________

Parent/Carer of: ________________________ **Class:** ____________________

APPENDIX G- Record of reviewing devices / internet sites

(Responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

APPENDIX H - School Technical Security and Password Policy

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of the IT Manager.

Technical Security

Air Balloon Hill Primary School will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that procedures approved within this policy are implemented. It will also ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the school / academy meets recommended technical requirements

- There will be regular reviews and audits of the safety and security of school academy technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted

- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff

- All users will have clearly defined access rights to school technical systems. The access rights available to groups of users will be recorded by the IT Manager and will be reviewed, at least annually.

- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. (See Password section below).

- The IT Manager is 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 (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)

- Mobile device security and management procedures are in place (where mobile devices are allowed access to school systems).

- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school system.

- The downloading of executable files and the installation of programmes on school devices by users is NOT allowed

- The Staff (and Volunteer) Acceptable Use Policy Agreement details the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.

- The Staff (and Volunteer) Acceptable Use Policy Agreement details the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.

- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.

- Personal data must not sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT Manager and will be reviewed, at least annually.

  - All school networks and systems will be protected by secure passwords that are regularly changed

  - The "master / administrator" passwords for the school systems, used by the the IT Manager must also be available to the Headteacher and kept in a secure place eg school safe.

- Passwords for new users, and replacement passwords for existing users will be allocated by the IT Manager.

- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

- Users will change their passwords at regular intervals – as described in the staff and pupil sections below

- requests for password changes should be authenticated by the IT Manager to ensure that the new password can only be passed to the genuine user.

Staff passwords

All staff users will be provided with a username and password by the IT Manager who will keep an up to date record of users and their usernames.

- Passwords must not personal information about the user that might be known by others
- The account should be "locked out" following six successive incorrect log-on attempts
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- Passwords should be different for systems used inside and outside of school
- A generic limited account logon can be used by early year's pupils due to the process of login for very young pupils this will be actively managed by the Teachers who use this facility.

Training / Awareness
It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss.

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-safety policy and Technical Security policy
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The IT Manager will ensure that full records are kept of:

- User IDs and requests for password changes
- User logins
- Security incidents related to this policy