APPLEBY PRIMARY SCHOOL
E-SAFETY POLICY

Name of School	**Appleby Primary School**
Policy review Date	**04/02/16**
Date of next Review	**04/02/17**
Who reviewed this policy?	

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

Contents

Appendices:

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Appleby Primary School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying.

- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of Appleby Primary School community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Appleby Primary School IT systems, both in and out of Appleby Primary School.

APPLEBY PRIMARY SCHOOL
E-SAFETY POLICY

Roles and responsibilities

Role	Key Responsibilities
Headteacher *Rachel Pearson*	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services including, filtered Internet Service. • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To receive regular monitoring reports from the Online Safety Co-ordinator • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure school website includes relevant information.
Online Safety Co-ordinator *Madeleine Hunter*	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate • To communicate regularly with the designated online safety Governor to discuss current issues, review incident logs and filtering/change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident

Role	**Key Responsibilities**
	• To ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Safeguarding governor (including online safety) *John Baxter*	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in online safety activities • The role of the online safety Governor will include: regular review with the online safety Co-ordinator.
Computing Curriculum Leader *Madeleine Hunter*	• To oversee the delivery of the online safety element of the Computing curriculum
Network Manager/technician *Systems IT*	• To report online safety related issues that come to their attention, to the Online Safety Coordinator • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis • That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of school technology is regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security

Role	Key Responsibilities
	and technical procedures
Data and Information Managers *Rachel Bousfield* *Debbie Parkin*	• To ensure that the data they manage is accurate and up-to-date • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • The school must be registered with Information Commissioner
Teachers	• To embed online safety in the curriculum • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff, volunteers and contractors.	• To read, understand, sign and adhere to the school staff Information Systems and Code of Conduct, and understand any updates annually. The Code of Conduct is signed by new staff on induction. • To report any suspected misuse or problem to the online safety coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology **Exit strategy** • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school.
Pupils	• Read, understand, sign and adhere to the Student E-safety Rules. To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school • To contribute to any 'pupil voice' / surveys that gathers information

Role	Key Responsibilities
	of their online experiences
Parents/carers	• To read, understand and promote the school’s E-Safety Rules with their child/ren • To consult with the school if they have any concerns about their children’s use of technology • To support the school in promoting online safety and endorse the E-Safety which includes the pupils’ use of the Internet and the school’s use of photographic and video images

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/ staffroom/ classrooms.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- E-Safety Rules discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Online Safety Coordinator acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority’s Designated Officer).

Review and Monitoring

The online safety policy is referenced within other school policies

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind students about their responsibilities through the E-Safety Rules;
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;

- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is monitored;
- has the educational filtered secure broadband connectivity through Systems IT;
- uses a filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- ensures network health through use of Sophos anti-virus software (from LGfL);
- Uses CumbriaGfL approved systems and secure email to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the System IT to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users ;
- Uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful;
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a username and password. The same credentials are used to access the school's network.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;

- Ensures all equipment owned by the school and connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted
- Our wireless network has been secured to appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.
- We require staff to change their passwords every 90 days

E-mail

This school

- Provides staff with an email account for their professional use, Cumbria Grid for Learning email and makes clear personal email should be through a separate account;
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- We use a number of System IT technologies to help protect users and systems in the school, including desktop anti-virus product Sophos plus direct email filtering for viruses.

Staff:

- Staff will use CGfL e-mail systems for professional purposes
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

APPLEBY PRIMARY SCHOOL
E-SAFETY POLICY

School website

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Cloud Environments

- Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil. Any exceptions must be approved by the Headteacher.
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, students & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be kept in the main office until home-time.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- Staff members may use their phones during school break times.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Storage, Synching and Access

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.

Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form annually;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- We do not take videos, photos or recordings of pupils on staff personal devices.
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;

- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

APPLEBY PRIMARY SCHOOL
E-SAFETY POLICY

Appendix 1

CODE OF CONDUCT FOR THE USE OF THE APPLEBY PRIMARY SCHOOL NETWORK, E-MAIL AND INTERNET FOLLOWING NETWORK GUIDELINES

This simplified code of conduct applies at all times, in and out of school hours, whilst using school IT equipment

You should:

- Only access websites that are appropriate to your education
- Respect the computer equipment and report any problems or damage to your teacher
- Respect copyright and trademarks (you cannot copy material without giving credit to the person or company that owns it)
- Respect the IT facility as a whole: Remember that it is a privilege, not a right, to use IT equipment

You must not:

- Download any music or video files under any circumstances unless approved by your teacher for educational purposes
- Visit any game or pornographic sites
- Stream video across the Network
- Use Chat sites such as MSN Messenger
- Searches must not be attempted for trivial or offensive material
- Complete or fill out any subscription forms
- Give your name, address, telephone number etc. for any other personal information about yourself or others to anyone
- Send offensive messages or pictures
- Download and run any executable files unless authorised by your teacher
- Intentionally waste resources thus preventing use by others
- Bypass web filter security to access restricted sites

Please note:

The consequences of disobeying any of these rules will be

- Disciplinary meeting with parents, or exclusion
- Restricted access to certain (pre-defined) educational sites
- If inappropriate you will be reported to the police

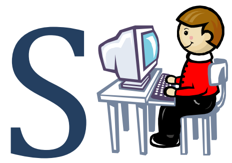
Appendix 2

E-SAFETY RULES

(Key Stage 1 & 2)

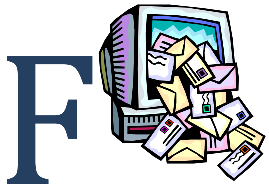
KEY STAGE 1

Think before you click



I will only use the Internet and email with an adult

I will only click on icons and links when I know they are safe



I will only send friendly and polite messages

If I see something I don’t like on a screen, I will always tell an adult

APPLEBY PRIMARY SCHOOL
E-SAFETY POLICY

KEY STAGE 2

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

Appendix 3

E-SAFETY FOR PUPILS WITH SPECIAL EDUCATIONAL NEEDS

This document covers some considerations regarding possible ways to support a generic group of children who may require additional support to move forward in safeguarding themselves.

- A fundamental part of teaching e-safety is to check pupil's understanding and knowledge of general personal safety issues. Some pupils may need additional teaching that includes reminders and explicit prompts to link their existing knowledge of 'how to keep safe' to the rules that will apply specifically to, for instance, internet use.
- Rules are very helpful to all pupils and it is important to achieve consistency of how rules can be applied
  - This is a difficult area for some pupils who usually learn the rules within certain contexts, but who will find it difficult to transfer these rules across environments, lessons or teachers. Schools need to consider whether a scheme or resources are applicable or accessible to all school situations where internet access may be possible
  - As consistency is so important for these pupils, there is a need to establish e-safety rules for school that are similar to those for home. Working with parents and sharing information with them would be relevant to all children, but this group especially
  - There will always be exceptions to rules and if this is the case, then these pupils will need to have additional explanations about why the rules might change in different situations i.e. why it is acceptable to give your name and address to an adult if lost in town, but not when using the internet
  - It might be helpful to consider presenting the rules as being linked to consequences such that you are teaching cause-effect rather than a list of procedures. This needs to be achieved carefully so as to use realistic and practical examples of *what might happen if…….*without frightening pupils

How rules are presented could be vital to help these pupils understand and apply some of the rules they need to learn

- Visual support is usually important to help most pupils' understanding but some areas of this topic are quite abstract in nature and difficult to represent visually i.e.
  - Uncomfortable
  - Smart
  - Stranger
  - Friend

  It might be helpful to ask pupils to produce a drawing or write a mini-class dictionary that describes and defines these words in their own terms

- Visual support can be useful but it is more likely that the pupils will respond to multi-media presentations of the rules such as interactive power-point slides, screensavers, spoken recordings of the main rules or sounds that they can associate with decisions they make while using the internet. The really useful thing is the repetition and practice that pupils can have with these which may not be so easy if spoken language were used
- If visual prompts are used to help remember the rules, the picture or image support needs to give the pupils some improved understanding about what the rule is about. It is quite easy to find attractive pictures that link to other abstract ideas not related to the internet use i.e. use of a compass to show 'lose track' of a search when a head looking confused is more like what happens.

This group of pupils are vulnerable to poor social understanding that may leave them open to risks when using the internet individually, but also when with peers

- It can be common for peers to set up scenarios or 'accidents' regarding what they look for on the internet and then say it was someone else who had done so. Adults need to plan group interactions carefully when raising awareness of internet safety
- Some pupils in this group may choose recreational internet activities that are perhaps simpler or aimed at pupils younger than themselves. By their very nature, these activities tend to be more controlled and less open to naïve mistakes. Staff need to plan how to manage pupils who may want to do the same as other peers but who may need small step teaching due to limited experiences with internet use

For various reasons, pupils with special educational needs may find it difficult to explain or describe events when using the internet

- Some pupils may find it easier to show adults what they have done i.e. replay, which will obviously have it's own issues for staff regarding repeating access
- Some pupils are very quick to click with the mouse and may not actually know what they did or how something happened. Gentle investigation will be more productive than asking many questions

Some may not be able to ask for help. Staff will need to know specific pupils well so that this can be addressed

- Pupils may need a system or help sounds to set up computers which will help them get adult attention. If pupils do not recognise that they need help, then adult supervision is the safe way to improve their recognition of this

Useful websites for resources

www.gridclub.com

www.kidsamrt.org.uk

www.thinkuknow.uk

Appendix 4

CONSENT

Gaining pupils’ and parents, agreement to the e-Safety rules is important but will require management. Many schools obtain this at the same time as checking home and emergency contact details annually.

To ensure clarity, the e-Safety rules appropriate to the age of the pupil should be included with the letter to parents.

It is important to start from the assumption that ICT and Internet use is everyday and essential for every child’s education. The agreement between parents and the school could include a phrase such as:

> ***All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.***

Where schools arranged purchase, rent or lease portable computers for use by pupils at home, a more comprehensive agreement is required.

Appleby Primary School

e-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupil and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed

Pupil:	*Form:*
Pupil's Agreement • I have read and I understand the school e-Safety Rules • I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times • I know that network and Internet access may be monitored.	
Signed:	***Date:***
Parent's Consent for Web Publication of Work and Photographs I agree that my son/daughters work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupils names **Parent's Consent for Internet Access** I have read and understood the school e-safety rules and give permission for my son/daughter to access the Internet. I understand that the school will take	

all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate this is a difficult task. I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from the use of the Internet facilities	
Signed:	***Date:***
Please print name:	
Please complete, sign and return to school	

Appendix 5

Appleby Primary School E-SAFETY CHECKLIST

Acceptable Use Policy

- **Does the school have an Acceptable Use Policy (AUP) for the use of its network? Is it regularly updated to take account of emerging technologies and events?**
- **Do all interested parties support the AUP: governors, senior management team, teaching staff, non-teaching staff, students and parents/carers**
- **Does the school send information to parents/carers regarding ICT use in schools?**
- **Have all pupils parents/carers, including mid term entrants, given their consent for their children to use the Internet in school? What action will the school take if consent is upheld?**
- **Do the school Anti-bullying and Behaviour Management policies make reference to electronic media and communication both inside and outside school?**
- **Does the school Staff Handbook / Staff Code of Conduct refer to electronic media and communication both inside and outside school?**
- **Does the school provide appropriate opportunities within a range of curriculum areas to teach Internet safety?**
- **Are there procedures in place to deal with 'disclosure' by a child of a personal nature as a result of Internet safety education? Has the school nominated a member of staff to be responsible for such issues?**
- **Have students and staff been made aware of their individual responsibility to protect the security and confidentiality of the schools network? This may include ensuring that usernames and passwords are not shared and workstations are not left unattended whilst logged on**
- **Does the school take reasonable steps to monitor pupils' and staff use of the Internet, email and/or chat rooms on a regular basis to ensure that inappropriate use is not being made?**
- **Have pupils and parents been advised that pupils' use of the Internet and email systems may be monitored and what procedures and sanctions are in place should misuse occur?**
- **Does the school adopt safe practices regarding the publication of the images and names of pupils and staff on its website?**
- **Is the AUP supported by clearly defined procedures and sanctions should misuse occur?**
- **Has the school nominated a member of staff who is responsible for Internet safety?**

APPLEBY PRIMARY SCHOOL
E-SAFETY POLICY

Internet Filtering

- **Does the school have Internet Filtering in place?**
- **If the school has adopted local control for some of its Internet filtering has the school nominated a "Filtering Administrator" that is responsible for appropriate filtering of the Internet in school?**
- **Has the school nominated a member of staff to be responsible for clearing local Internet cache servers (if present) of any inappropriate material that is reported and subsequently blocked by the filters**
- **Are pupils and staff aware of procedures for reporting accidental access to inappropriate materials on the Internet?**
- **Are there a range of sanctions or breaches of AUP? Are students aware of sanctions?**

Network Security

- **Does the school ensure that members of staff undertake to secure portable ICT equipment such as laptops and cameras when not in use? Are sanctions in place where staff fail to do so resulting in loss of equipment?**
- **Has the school deployed an appropriate level of security on its networks to ensure their reliability and prevent unauthorised access to systems and data?**
- **Has the school deployed sufficient security on any wireless networking to ensure that there is no unauthorised access to the school network?**
- **Is Antivirus protection provided on all machines? Is it regularly updated?**
- **Does the school ensure that its windows operating systems are regularly updated?**
- **Does the school possess sufficient software licences for the software installed on its network?**

Appendix 6

Prevent: Radicalisation and Extremism

Roles and Responsibilities of the Single Point of Contact (SPOC), The SPOC for Appleby Primary School is Rachel Pearson (Head Teacher), who is responsible for:

- Ensuring that staff of the school are aware that you are the SPOC in relation to protecting students/pupils from radicalisation and involvement in terrorism.

- Maintaining and applying a good understanding of the relevant guidance in relation to preventing students/pupils from becoming involved in terrorism, and protecting them from radicalisation by those who support terrorism or forms of extremism which lead to terrorism.

- Raising awareness about the role and responsibilities of Appleby Primary School in relation to protecting students/pupils from radicalisation and involvement in terrorism.

- Monitoring the effect in practice of the school's RE curriculum and assembly policy to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.

- Raising awareness within the school about the safeguarding processes relating to protecting students/pupils from radicalisation and involvement in terrorism.

- Acting as the first point of contact within the school for case discussions relating to students / pupils who may be at risk of radicalisation or involved in terrorism.

- Attending LA meetings as necessary and carrying out any actions as agreed.

- Sharing any relevant additional information in a timely manner.

Appendix 7

STAFF INFORMATION SYSTEMS CODE OF CONDUCT

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the *Online Safety Coordinator.*
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will follow the school's policy on use of mobile phones / devices at school
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.

APPLEBY PRIMARY SCHOOL
E-SAFETY POLICY

- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert *Appleby Primary School's* child protection officer member of staff if I feel the behaviour of any child may be a cause for concern.
- *Staff that have a teaching role only:* I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's information systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct

APPLEBY PRIMARY SCHOOL

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