Online Safety Policy (including E-Safety)

Adopted by Governing Body: 16.01.19

Signed: ……. Chair of Governors

Contents

Background and rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even truer for children, who are generally much more open to developing technologies than many adults. In many areas, technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Allowing or seeking unauthorised access to personal information
- Allowing or seeking unauthorised access to private data, including financial data
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive or addictive use which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures put in place to keep them safe) and so this policy also sets out how we educate children about the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Our school's e-safety policy has been written from a template provided by Worcestershire County Council.

Section A - Policy and leadership
This section begins with an outline of the **key people responsible** for developing our E-Safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of all users of ICT in our school. It goes on to explain **how we maintain our policy** and then to outline **how we try to remain safe while using different aspects of ICT**

A.1 Responsibilities
The school council now has a standing agenda item where discussions around issues relating to e-safety can be shared. When appropriate, our school e-safety coordinator attends meetings. Issues that arise are referred to other school bodies as appropriate and when necessary to bodies outside the school such as the Worcestershire Safeguarding Children Board (to be known as 'Safeguarding Partners' from Spring 2019).

A.1.1 Responsibilities: E-safety coordinator
Our e-safety coordinator is our IT coordinator, the person responsible to the head teacher and governors for the day to day issues relating to e-safety. The e-safety coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- receives reports of e-safety incidents as they occur and creates a log of incidents to inform future e-safety developments
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school IT technical staff
- meets regularly with the Head teacher to discuss current issues and review incident logs
- attends relevant meetings and committees of the governing body
- reports when necessary to Senior Leadership Team
- receives appropriate training and support to fulfil their role effectively

A.1.3 Responsibilities: Governors
Governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governor curriculum committee who will receive information about e-safety incidents and monitoring reports when appropriate. A member of the governing body has taken on the role of e-safety governor which involves:

- termly conversations with the E-Safety Co-ordinator with an agenda based on:
- monitoring of e-safety incident logs
- reporting to relevant Governors committee / meeting

A.1.4 Responsibilities: Head teacher and Deputy Head teacher

- The Head teacher is responsible for ensuring the safety (including e-safety) of all members of the school community, though the day to day responsibility for e-safety is delegated to the E-Safety Co-ordinator
- The Head teacher and deputy head teacher (Designated Safeguarding Lead) receives and reviews the weekly output from monitoring software and initiates action where necessary

- The head teacher and deputy head teacher will be familiar with the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff, including non-teaching staff. (see flow chart on dealing with e-safety incidents (included in section 2.6 below) and other relevant Local Authority HR / disciplinary procedures)

A.1.5 Responsibilities: classroom based staff

Teaching and Support Staff are responsible for ensuring that:

- they safeguard the welfare of children and refer child protection concerns using 'myconcern' our online reporting package: **this duty is on the individual, not the organisation or the school**.
- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices including the school's approach to the PREVENT agenda
- they have read, understood and signed the school's Acceptable Use Agreement for staff (see Appendix 1)
- they report any suspected misuse or problem to the E-Safety Co-ordinator
- they undertake any digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) in a fully professional manner and only using official school systems (see A.3.5)
- they embed e-safety issues in the curriculum and other school activities, also acknowledging the planned e-safety programme (see section C)

A.1.6 Responsibilities: ICT technician

The ICT Technician is responsible for ensuring that:

- the school's ICT infrastructure and data are secure and not open to misuse or malicious attack
- the school meets the e-safety technical requirements outlined in section B.2.2 of this policy (and any relevant Local Authority E-Safety Policy and guidance)
- users may only access the school's networks through a properly enforced password protection policy as outlined in the school's e-security policy
- shortcomings in the infrastructure are reported to the ICT technician or head teacher so that appropriate action may be taken.

A.2.1 Policy development, monitoring and review

This e-safety policy has been developed (from a template provided by Worcestershire County Council) by a working group made up of:

- *Head teacher*
- *School E-Safety Coordinator*
- *Deputy Head teacher*
- *E-safety governor*

Consultation with the whole school community has taken place through the following:

- *Dissemination to Staff*
- *School Council*
- *Governors curriculum committee meeting*
- *Parents and Carers*
- *Pupils*

Schedule for development / monitoring / review of this policy

The implementation of this e-safety policy will be monitored by the:
The E-Safety Co-ordinator, Headteacher, SLT & Governing Body
Monitoring will take place at regular intervals. This will be done through regular meetings between the e-safety co-ordinator and the headteacher.
The governing body will receive regular reports on the implementation of the e-safety policy (which will include anonymous details of e-safety incidents) as part of a standing agenda item with reference to safeguarding.
The e-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technology, new threats to e-safety or incidents that have taken place. Should serious e-safety incidents take place, the following external persons / agencies should be informed: Worcestershire Safeguarding Children Board e-safety representative, Local Authority Designated Officer, Worcestershire Senior Adviser for Safeguarding Children in Education or West Mercia Police.

A.2.2 Policy Scope

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

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, radicalisation or other e-safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school.

The school will deal with such incidents using guidance within this policy as well as associated behaviour, safeguarding and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

A.2.3 Acceptable Use Agreements

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems.

Acceptable Use Agreements are provided in Appendix 1 of this policy for:

- Pupils
- Staff (Volunteers are not permitted to access the school ICT system)
- Technical support personnel

Acceptable Use Agreements are signed by all pupils from Key Stage 1 upwards, where appropriate. Pupils re-sign these agreements annually.

All employees of the school sign when they take up their role in school and in the future if significant changes are made to the policy.

Parents sign once when their child enters the school. The parents' policy also includes permission for use of their child's image (still or moving) by the school, permission for their child to use the school's ICT resources (including the internet) and permission to publish their work.

Community users sign when they first request access to the school's wireless network.

Induction policies for all new members of staff include this guidance.

A.2.4 Self Evaluation

Evaluation of e-safety is an ongoing process and links to other self-evaluation tools used in school in particular to pre Ofsted evaluations along the lines of the Self Evaluation Form (SEF).

A.2.5 Whole School approach and links to other policies

This policy has strong links to other school policies as follows:

Core ICT policies

E-Safety Policy	How we strive to ensure that all individuals in school stay safe while using Learning Technologies. The e-safety policy constitutes a part of the ICT policy.
Data Protection Policy	How we categorise, store and transfer sensitive and personal data and protect school systems. This links strongly and overlaps with the e-safety policy.

Other policies relating to e-safety

Anti-bullying	How our school strives to eliminate bullying – link to cyber bullying

PSHE	E-Safety has links to staying safe
Safeguarding	Safeguarding children electronically is an important aspect of E-Safety. ***The e-safety policy forms a part of the school's safeguarding policy***
Behaviour	Positive strategies for encouraging e-safety and sanctions for disregarding it.
Safe and Appropriate Use of Images	**WCC guidance to support the safe and appropriate use of images in schools and settings**

A.2.6 Users shall not visit Internet sites, make, post, download, upload, transfer data, communicate or pass on material, remarks, proposals or comments that contain or relate to:

- **child sexual abuse images (illegal - The Protection of Children Act 1978)**
- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)**
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- 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

Additionally the following activities are also considered unacceptable on ICT equipment or infrastructure provided by the school:

- Using school systems to undertake transactions pertaining to a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by CIS Schools Filtering and / or the school

- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files that causes network congestion and hinders others in their use of the internet)
- On-line gambling and non-educational gaming
- On-line shopping / commerce, unless directly related to school business
- Use of social networking sites (other than in the school's learning platform or sites otherwise permitted by the school)

If members of staff suspect that misuse might have taken place – whether or not it is evidently illegal (see above) - it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. Please see Appendix 2.

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 indicated on the following pages:

	Refer to:					**Inform:**	**Action:**		
Pupil sanctions *Schools should edit this table as appropriate to their institution.* *The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.*	Class teacher	E-safety coordinator	Refer to head teacher	Refer to Police	Refer to e -safety coordinator for action re	Parents / carers	Remove of network / internet access rights Warning		Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✔	✔	✔	✔	✔	✔	✔	✔	✔

Unauthorised use of non-educational sites during lessons	✔				✔				
Unauthorised use of mobile phone / digital camera / other handheld device	✔					✔	✔		
Unauthorised use of social networking / instant messaging / personal email	✔	✔			✔	✔		✔	
Unauthorised downloading or uploading of files	✔						✔	✔	
Allowing others to access school network by sharing username and passwords	✔	✔	✔		✔		✔	✔	
Attempting to access the school network, using another pupil's account	✔				✔		✔		
Attempting to access or accessing the school network, using the account of a member of staff	✔		✔		✔	✔		✔	
Corrupting or destroying the data of other users	✔		✔		✔	✔	✔	✔	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✔	✔	✔		✔	✔	✔	✔	
Continued infringements of the above, following previous warnings or sanctions	✔	✔	✔			✔	✔		✔
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✔		✔					✔	
Using proxy sites or other means to subvert the school's filtering system	✔	✔	✔		✔	✔	✔	✔	
Accidentally accessing offensive or pornographic material and failing to report the incident	✔	✔			✔	✔			
Deliberately accessing or trying to access offensive or pornographic material	✔	✔	✔		✔	✔	✔		✔
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✔		✔		✔		✔		

Staff sanctions

Schools should edit this table as appropriate to their institution.

The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.

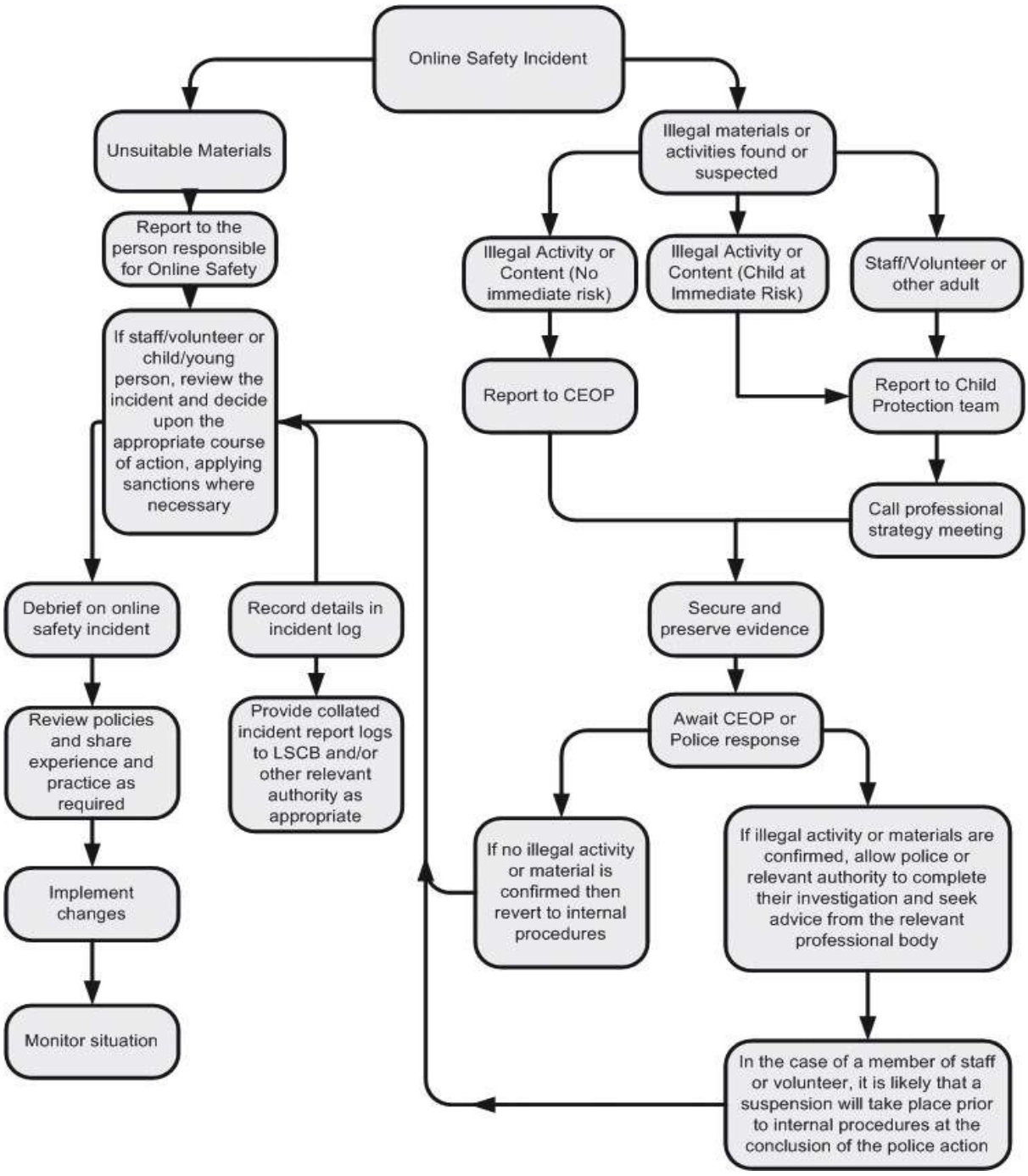
	Refer to:					**Action:**		
	ICT Co -ordinator	Head teacher	Local Authority / HR	Police	Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✔	✔	✔	✔		✔	✔
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✔	✔				✔		
Unauthorised downloading or uploading of files	✔				✔	✔		
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	✔	✔			✔	✔	✔	
Careless use of personal data e.g. holding or transferring data in an insecure manner	✔	✔	✔		✔	✔		✔
Deliberate actions to breach data protection or network security rules	✔	✔	✔		✔	✔	✔	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✔	✔				✔	✔
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✔	✔				✔	✔	
Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students / pupils	✔	✔			✔			
Actions which could compromise the staff member's professional standing	✔	✔						

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✔	✔				✔		
Using proxy sites or other means to subvert the school's filtering system	✔				✔	✔		✔
Accidentally accessing offensive or pornographic material and failing to report the incident	✔	✔			✔	✔		
Deliberately accessing or trying to access offensive or pornographic material	✔	✔	✔		✔	✔	✔	✔
Breaching copyright or licensing regulations	✔					✔		
Continued infringements of the above, following previous warnings or sanctions	✔	✔			✔			✔

A.2.7 Reporting of e-safety breaches

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

Particular care should be taken if any apparent or actual misuse appears to involve illegal activity listed in section A.2.6 of this policy



A.3.1 Use of hand held technology (personal phones and hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:
    - ✓ School land-line will be used in lesson time only in an emergency or extreme circumstances
    - ✓ Members of staff are free to use these devices outside teaching time and away from pupils.

- ✓ A school mobile phone is available for all professional use (for example when engaging in off-site activities). Members of staff should **not** use their personal devise for school purposes except in an emergency.

- Pupils are not currently permitted to bring their personal hand held devices into school. These have to be handed in at the beginning of the day and not collected until the end of the day.

	Staff / adults				Pupils			
Personal hand held technology *It is important that schools review this table in the light of principles agreed within their own establishment.*	Allowed	Allowed at certain	Allowed for selected	Not allowed	Allowed	Allowed at certain	Allowed with staff	Not allowed
Mobile phones may be brought to school	✔							✔
Use of mobile phones in lessons				✔				✔
Use of mobile phones in social time		✔						✔
Taking photos on personal phones or other camera devices				✔				✔
Use of hand held devices e.g. PDAs, gaming consoles	✔						✔	

A.3.2 Use of communication technologies

A.3.2a - Email

Access to email is provided for all users in school via Office 365 which is managed by in house ICT staff.

These official school email services may be regarded as safe and secure and are monitored.

Staff and pupils should use only the school email services to communicate with others when in school, or on school systems (e.g. by remote access)

- Users need to be aware that email communications may be monitored
- Pupils normally use only a class email account to communicate with people outside school and with the permission / guidance of their class teacher
- A structured education program is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email
- Staff may only access personal email accounts on school systems regarding work related issues
- Users must immediately report to their class teacher / e-safety coordinator – in accordance with the school policy (see sections A.2.6 and A.2.7 of this policy) - the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and they must not respond to any such email.

	Staff / adults				Pupils			
Use of Email *It is important that schools review this table in the light of principles agreed within their own establishment.*	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Use of personal email accounts in school / on school network				✔				✔
Use of school email for personal emails				✔				✔

A.3.2b - Social networking (including chat, instant messaging, blogging etc)

	Staff / adults				Pupils			
Use of social networking tools *It is important that schools review this table in the light of principles agreed within their own establishment.*	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Use of non-educational chat rooms etc				✔				✔

Use of non-educational instant messaging				✔				✔
Use of non-educational social networking sites				✔				✔
Use of non-educational blogs				✔				✔

A.3.2c – Videoconferencing Not applicable.

A.3.3 Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. (See section C). In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; **the personal equipment of staff should not be used for such purposes.**
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Staff should be aware of pupils for whom it has been deemed inappropriate to take and share / publish their photograph (e.g. some looked after children)
- Pupils must not take, use, share, publish or distribute images of others without their permission

See also the following section (A.3.4) for guidance on publication of photographs

A.3.4 Use of web-based publication tools

A.3.4a - Website (and other public facing communications)

Our school uses the public facing website only for sharing information with the community beyond our school. This includes, from time-to-time, celebrating work and achievements of children. All users are required to consider good practice when publishing content.

- Personal information will not be posted on the school website and only official email addresses will be used to identify members of staff (never pupils).
- Only pupil's first names will be used on the website, and only then when necessary.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
  - ✓ pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
  - ✓ staff to be aware of positioning when taking photographs

- ✓ written permission from parents or carers will be obtained before photographs of pupils are published on the school website (see section A.2.3 and Appendix 1)

Pupil's work can only be published with the permission of the pupil and parents or carers. (see section A.2.3 and Appendix 1)

A.3.4b – Learning Platform Not applicable

A.3.5 Professional standards for staff communication

In all aspects of their work in our school, teachers abide by the broad **Professional Standards for Teachers** laid down by the TDA effective from September 2012: http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf.

Teachers translate these standards appropriately for all matters relating to e-safety.

Any digital communication between staff and pupils or parents / carers (email, chat, learning platform etc) must be professional in tone and content.

- These communications may only take place on official (monitored) school systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

The views and experiences of pupils are used to inform this process also.

Section B. Infrastructure

B.1 Password security

The school's e-safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of school (see section C of this policy)

B.2.1 Filtering

The School uses Visigo provided by Smoothwall, which is monitored off site by artificial intelligence 24/7. If a high-level breach occurs the school will be called within 30 minutes.

B.2.1a - Introduction

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. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a school we buy our connection from Worcestershire County Council, however the filtering service is purchased from CIS.

B.2.1b - Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the **esafety coordinator** (with ultimate responsibility resting with the **head teacher and governors**). They manage the school filtering in line with this policy and keep logs of changes to and breaches of the filtering system.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the standard Worcestershire school filtering service must

- be reported to a second responsible person (the head teacher) within the time frame stated in section A.1.3 of this policy

All users have a responsibility to report immediately to class teachers / e-safety coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

B.2.1c - Education / training / awareness

Pupils are made aware of the importance of filtering systems through the school's e-safety education programme (see section C of this policy).

Staff users will be made aware of the filtering systems through:

- signing the Acceptable Use Agreement (as part of their induction process)
- briefing in staff meetings, training days, memos etc. (timely and ongoing).

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions / newsletter etc.

B.2.1d - Changes to the filtering system

Where a member of staff requires access to a website that is blocked for use at school, the process to unblock is as follows:

- The teacher makes the request to the ICT Technician.
- The E-safety co-ordinator checks the website content to ensure that it is appropriate for use in school.

THEN

- If agreement is reached, the ICT Technician liaises with CIS by filling out a change request form.
- The Broadband helpdesk will endeavour to unblock the site within 24 hours. This process can still take a number of hours so teaching staff are required to check websites in advance of teaching sessions.
- School Improvement Service Learning Technologies staff may then be notified of websites that have been unblocked to review them in partnership with the Broadband Team. If sites are found to not be appropriate, access will be discussed with the school and then removed.

The ICT Technician will need to apply a rigorous policy for approving / rejecting filtering requests. This can be found in Appendix 3 but the core of this should be based on the site's content:

- The site promotes equal and just representations of racial, gender, and religious issues.

  The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.
- The site does not link to other sites which may be harmful / unsuitable for pupils.

B.2.1e - Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment.

Monitoring takes place as follows:

- The E-safety Co-ordinator reviews the monitoring console captures weekly.
- Potential issues are referred to an appropriate person depending on the nature of the capture.
- Teachers are encouraged to identify in advance any word or phrase likely to be picked up regularly through innocent use (e.g. 'goddess' is captured frequently when a class is researching or creating presentations on the Egyptians) so that the word can be allowed for the period of the topic being taught.

B.2.1f - Audit / reporting

Filter change-control logs and incident logs are made available to:

- the Safeguarding governor within the timeframe stated in section A.1.3 of this policy
- the Worcestershire Safeguarding Children Board on request

This filtering policy will be reviewed, with respect to the suitability of the current provision, in response to evidence provided by the audit logs.

B.2.2 Technical security

This is dealt with in detail in the school's System and Data Security Policy (to be produced).

B.2.3 Personal data security (and transfer)

This is dealt with in detail in the school's System and Data Security Policy (to be produced). Teachers frequently discuss issues relating to data security and how it relates to staying safe in and out of school (see section C of this policy).

Section C. Education

C.1.1 E-safety education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the continuous help and support of the school to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

E-Safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of ICT, PHSE and other lessons as appropriate to the needs of pupils. This is regularly revisited, covering the use of ICT and new technologies both in school and outside school.
- Key e-safety messages will be reinforced through further input via assemblies and pastoral activities, as well as informal conversations when the opportunity arises.
- Pupils will be helped to understand how to adopt safe and responsible use of ICT both within and outside school.

- In lessons where internet use is pre-planned, it is best practice that 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 (refer to Acceptable Use Agreements relevant to Key Stages).

- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit, encouraging them to discuss anything of which they are unsure and implementing the expected sanctions and/or support as necessary.

- Pupils will be made aware of what to do should they experience anything, while on the Internet, which makes them feel uncomfortable.

C.1.2 Information literacy

- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information. Best practice would include:
  - ✓ Checking the likely validity of the URL (web address)
  - ✓ Cross checking references (Can they find the same information on other sites?)
  - ✓ Checking the pedigree of the compilers / owners of the website
  - ✓ Referring to other (including non-digital) sources
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require
- *We use the resources on CEOP's Think U Know site as a basis for our e-safety education http://www.thinkuknow.co.uk/teachers/resources/.*

C.1.3 The contribution of the children to e-learning strategy

It is our general school policy to encourage pupils to play an active role in shaping the way our school operates and this is very much the case with our e-learning strategy. Pupils often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology (especially rapidly developing technology such as mobile devices) could be helpful in their learning.

Pupils play a part in monitoring this policy (see section A.1.1)

C.2 Staff training

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

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- Some staff may identify e-safety as a training need within the performance management process.
- 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 policies which are signed as part of their induction
- The E-safety co-ordinator is CEOP trained.
- The E-Safety Coordinator will receive regular updates through attendance at local authority or other training sessions and by reviewing guidance documents released by the DfE, OFSTED, the local authority, the WSCB and others.
- A representative body of staff have been involved in the creation of this e-safety policy and are therefore aware of its content
- The E-Safety Coordinator will provide advice, guidance and training as required to individuals as required on an ongoing basis.
- External support for training, including input to parents/carers, is sought from appropriately qualified persons when required.

C.3 Governor training

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

- Attendance at training provided by the Local Authority (Governor Services or School Improvement Service), National Governors Association or other bodies.
- Participation in school training / information sessions for staff or parents

The e-safety governor works closely with the e-safety coordinator and reports back to the full governing body (see section A.1.3)

C.4 Parent and carer awareness raising

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 and regulation of the children's on-line experiences. Parents/carers often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to family members and carers through:

- Letters, newsletters, website

- Parents/carers evenings
- Parents/carers workshops

C.5 Wider school community understanding

Community Users are not permitted to access school ICT systems / website / learning platform.

Appendix 1a – Acceptable Use Agreement pupil (version 1)

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computer
- I will only use activities if an adult says it is OK.
- I will take care of the computer and other equipment
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will turn off the monitor and tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

I understand these computer rules and will do my best to keep them

My name:	
Signed (child):	
OR Parent's signature:	
Date:	

Appendix 1b – Acceptable Use Agreement pupil (version 2)

I understand that while I am a member of Rigby Hall School I must use technology in a responsible way.

For my own personal safety:

- I understand that when I use the internet I will be supervised and monitored.
- I will keep my password safe and will not use anyone else's (even with their permission).
- I will keep my own personal information safe, as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

For the safety of others:

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others.
- I will not take or share images of anyone without their permission.

For the safety of the school:

- I will not try to access anything illegal.
- I will not download anything that I do not have the right to use.
- I will only use my own personal device if I have permission and use it within the agreed rules.
- I will not deliberately bypass any systems designed to keep the school safe.
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes of any type on devices belonging to the school without permission.
- I will only use social networking, gaming and chat through the sites the school allows

KS3/4 Pupil Acceptable Use Agreement Form

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

Name:	
Signed:	
Date:	

Appendix 1c - Acceptable Use Agreement – staff & volunteer

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, learning platform) out of the school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down in the e-safety policy.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident of which I become aware, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school/academy's policy on the use of digital images. I will not use my personal equipment to record these images.
- Where images are published (e.g. on the school website / learning platform) I will ensure that it will not be possible to identify by name, or other personal information, those who are featured. (see section A.3.3 of the e-safety policy)
- I will only use chat and social networking sites in school in accordance with the schools policies. (see section A.3.2 of the e-safety policy)
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (see sections A.3.1 and A.3.2 of the e-safety policy)
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school *and the local authority* have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will only use my personal mobile ICT devices as agreed in the e-safety policy (see section A.3.1) and then with the same care as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems except in an emergency (A.3.2).
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up in accordance with relevant school policies (Maintained and subscribing establishments see CIS Schools Systems and Data Security advice).
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist or radical (radicalisation) material, adult pornography covered by the Obscene Publications

Act) or inappropriate or may cause harm or distress to others. I will not 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 not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/ LA Personal Data Policy. **I understand that where personal data is transferred outside the secure school network, it must be encrypted.**
- I will not take or access pupil data, or other sensitive school data, off-site without specific approval. If approved to do so, I will take every precaution to ensure the security of the data,
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school/academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in the school, but also applies to my use of school ICT systems and equipment out of the school and to my use of personal equipment in the school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and/or the Local Authority and/or other relevant bodies including, in the event of illegal activities, the involvement of the police (see section A.2.6).

I have read and understand the above and agree to use the school ICT systems (both in and out of the school) within these guidelines.

Staff / volunteer Name:	
Signed:	
Date:	

Appendix 1d - Acceptable Use Agreement and permission forms – parent / carer

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure that:

- Young people will be responsible users and stay safe while using ICT (especially the internet).
- School ICT 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 ICT to enhance their learning and will, in return, expect them to agree to be responsible users.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of their work.

Child's name	
Parent's name and signature	
Date:	

Permission for my child to use the internet and electronic communication

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

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 and responsible use of ICT – both in and out of the school

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 Agreement.

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.

Parent's signature:	
Date:	

Permission to use digital images (still and video) of my child

This is part of the school welcome pack and held by the school administration.

The use of digital images (still and video) plays an important part in learning activities. Pupils and members of staff may use the school's digital cameras/ipads to record evidence of activities in lessons and out of the school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. The school will also ensure that when images are published, the young people cannot be identified by name.

Parents/carers complete a permission form as part of the school welcome pack and a summary list is kept updated at all times.

Permission to publish my child's work (including on the internet)

It is our school's policy, from time to time, to publish the work of pupils by way of celebration. This includes on the internet; via the website *and in the learning platform.*

Parents/carers complete a permission form as part of the school welcome pack and a summary list is kept updated at all times.

Appendix 1e - Acceptable Use Agreement – community user

You have asked to make use of our school's ICT facilities. Before we can give you a log-in to our system we need you to formally agree to use the equipment and infrastructure responsibly.

For my professional and/or personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, of which I become aware, to a member of the school's staff.

I will be responsible in my communications and actions when using the school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files or data, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist or radical material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not 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 described above.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, except with the specific approval of the school.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I have read and understand the above and agree to use the school ICT systems (both in and out of the school) within these guidelines. I understand that failure to comply with this agreement will result in my access to the school ICT systems being withdrawn, that further actions will be taken in the event illegal activity, and that I may be held liable for any damage, loss or cost to the school as a direct result of my actions.

Community user Name:	
Signed:	
Date:	

Appendix 2 - Guidance for Reviewing Internet Sites

This guidance is intended for use when the school needs 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 typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc.

Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case please refer to the Flowchart for responding to online safety incidents and report immediately to the police. Please follow all steps in this procedure:

- 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. *This will automatically be done for you if you are using Policy Central from Forensic Software or other monitoring software.* 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
    - Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.
- It is important that all of the above steps are taken as they will provide an evidence trail for the group, 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 group for evidence and reference purposes.

A sample document for recording the review of and action arriving from the review of potentially harmful websites can be found on the next page

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 3 – Criteria for website filtering

A. ORIGIN - What is the website's origin?

- The organisation providing the site is clearly indicated.
- There is information about the site's authors ("about us", "our objectives", etc.)
- There are contact details for further information and questions concerning the site's information and content.
- The site contains appropriate endorsements by external bodies and/or links to/from well-trusted sources

B. CONTENT - Is the website's content meaningful in terms of its educational value?

- The content is age-appropriate
- The content is broadly balanced in nature, and does not appear unduly biased, partisan or unreliable
- The site is free of spelling mistakes, grammatical errors, syntax errors, or typos.
- **The site promotes equal and just representations of racial, gender, and religious issues.**
- **The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.**
- **The site does not link to other sites which may be harmful / unsuitable for the pupils**
- The content of the website is current.

C. DESIGN - Is the website well designed? Is it / does it:

- appealing to its intended audience (colours, graphics, layout)?
- easy to navigate through the site - links are clearly marked etc?
- have working links?
- have inappropriate adverts?

D. ACCESSIBILITY - Is the website accessible?

- Does it load quickly?
- Does the site require registration or passwords to access it?
- Is the site free from subscription charges or usage fees?

Appendix 4 - Supporting resources and links

The following links may help those who are developing or reviewing a school e-safety policy.

General

South West Grid for Learning "SWGfL Safe" - http://www.swgfl.org.uk/Staying-Safe

Child Exploitation and Online Protection Centre (CEOP) http://ceop.police.uk/

ThinkUKnow http://www.thinkuknow.co.uk/

ChildNet http://www.childnet.com/

InSafe http://www.saferinternet.org/

Byron Reviews ("Safer Children in a Digital World") - https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Becta – various useful resources now archived
http://webarchive.nationalarchives.gov.uk/20101102103654/http:/www.becta.org.uk

London Grid for Learning - http://www.lgfl.net/esafety/Pages/education.aspx?click-source=nav-esafety

Northern Grid - http://www.digitallyconfident.org

National Education Network - http://www.nen.gov.uk/e-safety/

WMNet – http://www.wmnet.org.uk

EU kids Online - http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/Home.aspx

Cyber Bullying

Teachernet "Safe to Learn – embedding anti-bullying work in schools" (Archived resources)

http://tna.europarchive.org/20080108001302/http://www.teachernet.gov.uk/wholeschool/academy/behaviour/tacklingbullying/cyberbullying/

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org - http://www.cyberbullying.org/

CyberMentors: young people helping and supporting each other online - http://www.cybermentors.org.uk/

Prevent Duty -
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

Social networking

Digizen – "Young People and Social Networking Services": http://www.digizen.org/socialnetworking/

Get Safe On-line - https://www.getsafeonline.org/social-networking

Connect Safely - Smart socialising: http://www.connectsafely.org/

Mobile technologies

"How mobile phones help learning in secondary schools":

http://archive.teachfind.com/becta/research.becta.org.uk/upload-dir/downloads/page_documents/research/lsri_report.pdf

"Guidelines on misuse of camera and video phones in school/academies"
http://www.dundeecity.gov.uk/dundeecity/uploaded_publications/publication_1201.pdf

Data protection and information handling

Information Commissioners Office - Data Protection:

http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx

Digital Parenting - http://www.vodaphone.com/parents

http://www.digitalparenting.ie/

https://www.commonsensemedia.org/

Links to other resource providers

SWGfL has produced a wide range of information leaflets and teaching resources, including films and video clips – for parents and school/academy staff. A comprehensive list of these resources (and those available from other organisations) is available on the "SWGfL Safe" website: http://www.swgfl.org.uk/staying-safe

BBC Webwise: http://www.bbc.co.uk/webwise/

Kidsmart: http://www.kidsmart.org.uk/default.aspx

Know It All - http://www.childnet-int.org/kia/

Cybersmart - http://www.cybersmartcurriculum.org/home/

Internet Watch Foundation: http://www.iwf.org.uk

Digizen – cyber-bullying films: http://old.digizen.org/cyberbullying/film.aspx

Appendix 5 - Glossary of terms

AUA	Acceptable Use Agreement – see templates earlier in this document
Becta	British Educational Communications and Technology Agency (former government agency which promoted the use of information and communications technology – materials and resources are archived and still relevant)
CEOP	Child Exploitation and Online Protection Centre (part of UK Police), dedicated to protecting children from sexual abuse. Providers of the Think U Know programmes.
DfE	Department for Education
FOSI	Family Online Safety Institute
ICT	Information and Communications Technology
ICT Mark	Quality standard for school provided by NAACE for DfE
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
IWF	Internet Watch Foundation
JANET	Provides the broadband backbone structure for Higher Education and for the National Education Network and Regional Broadband Consortia
KS1; KS2	KS1 = years 1 and 2 (ages 5 to 7) KS2 = years 2 to 6 (age 7 to 11)
LA	Local Authority
LAN	Local Area Network
Learning platform	An online system designed to support teaching and learning in an educational setting
LSMIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (eg WMNet) to provide the safe broadband provision to school/academys across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PHSE	Personal, Health and Social Education
SRF	Self Review Framework – a tool maintained by Naace used by school/academies to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark
SWGfL	South West Grid for Learning – the Regional Broadband Consortium of SW Local Authorities and recognised authority on all matters relating to e-safety (on whose policy this one is based)
URL	Universal Resource Locator – a web address

WMNet	The Regional Broadband Consortium of West Midland Local Authorities – provides support for all school/academys in the region and connects them all to the National Education Network (Internet)
WSCB	Worcestershire Safeguarding Children Board (the local safeguarding board)

Reporting Log Group

Time	Incident	Action taken		Incident Reported by	Signature
		What?	By whom?		

	Date								

Appendix 7 Guidance to support the safe and appropriate use of images in schools and settings

Based on:

Safeguarding Children and Safer Recruitment in Education – *Consultation version 2010*

Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings – *DCSF March 2009*

Data Protection Good Practice Note: Taking Photographs in School – *Information Commissioner's Office 26th October 2007*

Please ensure that all staff are given copies of this guidance and made aware of school policy

Contacts:

Denise Hannibal, Senior Advisor, Safeguarding Children in Education dhannibal@worcestershire.gov.uk

Cath Ellicott, Early Years and Childcare Manager

CEllicott@worcestershire.gov.uk,

Appendix 8 Social Networking Teacher Agreement

For the protection of yourself, your school community and your establishment:

- Ensure that all your privacy settings are set to 'Friends Only'. Go to your Account Settings and make sure that the Custom Settings are highlighted and that these show that status, photos and posts are set to 'Friends Only'.

- Consider what information you have on your info page and your profile picture. Including brief information and an unidentifiable picture, e.g. sunset, will assist in making your profile indistinctive.

- Be careful what photographs you include on your profile. Once these are uploaded, they are very difficult to remove and, using image editing software, they can be altered and merged with other more distasteful images.

- If you have professional and social 'friends' on Facebook or other social networking sites, using the group list feature will ensure that you can distinguish what type of information you send to particular groups.

- Do not accept pupils (even those that have recently left the school), parents or carers as 'friends'.

- Do not use Facebook or other social networking sites in any way that might bring your professional status or your school into disrepute.

- Taking charge of your digital reputation is important, as unprofessional posts or images will lead to disciplinary action and possible failure to gain employment in the future.

- Do not post or upload photographs relating to colleagues, pupils or parents. Objection to such posts can cause friction in your school and make your working environment uncomfortable.

- Do not post or upload photographs related to school-based or extra-curricular activities and do not make specific reference to your school in any post as comments may be misconstrued and result in inappropriate responses.

- Be aware of any spam or potential virus risks sent via rogue posts. It is advisable to check with anti-virus firms if you get any suspicious requests or posts.

- If you are alerted to any negative or unscrupulous information about yourself, colleagues or your school on Facebook or other social networking sites, inform your headteacher. Further advice to help with cyberbullying incidents etc., can be gained from help@saferinternet.org.uk (0844 3814772) or a professional association such as your Trade Union.

- ***I understand the implications of using Facebook and other social networking sites for my own protection and professional reputation, as well as the impact that my use can have on my school community and establishment.***
- ***I understand that injudicious use of social networking may lead to disciplinary action.***
- ***I agree to take all possible precautions as outlined above.***

Name		***Date***	

Appendix 9 Loaned Device User Agreement

Staff member: Date:

Device Make: Model : Serial Number :

The laptop/device detailed above is loaned to Xxxxxxxxxxx Xxxxxxxxxx for the duration of their employment at Rigby Hall School subject to the following terms and the school Acceptable Use Agreement.

The iPad/mobile device remains the property of the School and must be returned at the end of the contracted period of employment with the School and, if required, during a planned or prolonged absence.

1. The laptop/device is for the **work related** use of the named member of staff to which it is issued.

2. Only software/apps installed at the time of issue or software/apps purchased by and licensed to Rigby Hall School may be installed on the machine.

3. The laptop/device remains the property of the School throughout the loan period, however the member of staff to which it is issued **will** be required to take responsibility for its care and safe keeping.

4. If left unattended the laptop/device must be securely stored. It must **never** be left unattended even for a short period in a car, including in a locked boot.

5. Due regard must be given to the security of the computer if using other forms of transport.

6. In order to ensure the schools compliance with the Data Protection Act and to avoid breaches of confidentiality, under no circumstances should students be allowed to use the staff laptops/devices if not directly supervised by a member of staff. Staff should also be cautious when using the computer away from school particularly with files which may contain personal student data, including images.

7. The equipment must be docked in the school charging and syncing cabinet at least once per week to ensure updates and new software are distributed. Staff should record this action in the log provided with the syncing cabinet.

8. The laptop/device will be recalled from time to time for routine maintenance / upgrade and monitoring.

Prohibited Uses

Images of other people, including children, may only be made with the permission of the person, or parents of the child, in the photograph.

The laptop/device is a professional tool designed to enhance classroom practice. It is not for personal use, e.g. Facebook or other social networking sites or on-line shopping, and should remain in school unless permission is sought from the ICT Co-ordinator or Head Teacher.

Lost, Damaged or Stolen laptop/device

If the laptop/device is lost, stolen or damaged, the ICT Co-ordinator or Head Teacher must be informed immediately and a charge may be levied depending on the circumstances.

I have read and agree to the terms and conditions in this agreement.
I undertake to take due care of the laptop or device and return it immediately upon request.

Signed: _____

Date: _____

This policy should be read in conjunction with the school Safeguarding Policy and Procedures (including Child Protection). All our practice and activities must be consistent and in line with the Safeguarding Policy and Procedures noted above. Any deviations from these policies and procedures should be brought to the attention of the Headteacher so that the matter can be addressed.