Crabbs Cross Academy

Online Safety Policy including Acceptable Use Agreements and Protocols for the Internet

Date of current review:	September 2020
Date of next review:	September 2021
Headteacher:	Sarah Shakles
Online Safety Lead:	Kim Power
Chair of Governors:	Jon Hughes

Contents

1. Rationale 4

2. Aims 5

3. Roles and Responsibilities 5

3.1 Online Safety Coordinator Role and Responsibilities 5

3.2 Governors Responsibilities 6

3.3 Headteacher responsibilities 6

3.4 Responsibilities: Classroom based staff 6

3.5 Responsibilities: ICT Technician 6

4. Policy Development, Monitoring and Review 7

4.1 Schedule for development / monitoring / review of this policy: 7

5. Network security and monitoring 7

5.1 Filtering 8

5.2 Passwords 8

5.3 Mobile technologies (see also Section 8) 8

5.4 Online learning technologies 8

6. Online Safety Awareness and training 9

6.1 Acceptable Use of the Internet 9

6.2 Email 9

6.3 Staff 10

7. Online Safety Training 10

7.1 Staff 10

7.2 Governors 10

7.3 Parent and Carer Awareness raising 10

7.4 Pupils 11

7.5 Online Safety Education 11

7.6 Information Literacy 12

8. Use of other communication and mobile technologies 12

8.1 Mobile phones 12

8.2 Emails 12

8.3 Use of Internet networking sites eg Facebook 13

9. Publishing of Content via digital resources or the internet 13

9.1 Copyright Issues 14

9.2 Use of the school's Internet facility by visitors and guests 14

10. Responding to incidents of inappropriate or undesirable use 14

10.1 Unintentional exposure of children to inappropriate content 14

10.2 Intentional access of undesirable content by children 14

10.3 Intentional access to undesirable content by adults 14

10.4 Reporting of online safety breaches 14

11. Disposal of ICT equipment 15

Appendix 1 16

Appendix 2 17

Appendix 3 18

Appendix 4 19

Appendix 5 20

Crabbs Cross Academy 20

Acceptable Use Agreement for Staff and Volunteers 20

Appendix 6 22

Acceptable Use Agreement for Teachers regarding the use of Facebook or other similar Social Networking sites. 22

Appendix 7 Guidance for Reviewing Internet Sites 23

Appendix 8 Criteria for Website Filtering 24

Appendix 9 Supporting resources and links 25

Appendix 10 Glossary of Terms 26

Online Safety Policy including
Acceptable Use Agreements and
Protocols for the Internet

The school policy for Online Safety, including Acceptable Use Agreements and Protocols for the use of the internet reflects the consensus of opinion of the whole teaching staff and has the full agreement of the Governing Body.

1. Rationale

The school and its partner agencies are committed to ensuring that children and young people are safeguarded whilst using information and communication technology (ICT).

"Children and young people have embraced new technologies as a source of information, education and entertainment. The use of digital technology has been completely normalized and it is now fully integrated into their daily lives. Children are using technology in new and exciting ways, enhancing and enriching their lives with the many tools on offer".

"ICT can offer many positive educational and social benefits to young people but unfortunately there are some dangers. As in any other area of life, children and young people are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies."

Signposts to e-safety Becta 2007

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 or other online 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 and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

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

Computing Policy	How Computing is taught, used, managed, resources and supported in our school.
Safeguarding Policy	Safeguarding children electronically is an important aspect of Online Safety. The Online Safety policy forms a part of the school's safeguarding policy.
Behaviour	Positive strategies for encouraging online safety and sanctions for disregarding it.
PSHE	Online Safety links to the PSHE curriculum, which teaches children how to stay safe.
Computing and Online Safety progression of skills	Documents detailing computing skills and how these progress through different year groups and curriculum coverage.

2. Aims

This policy is part of a suite of online safety documents and strategies developed:

- to ensure that pupils are provided with as safe and secure learning technologies and internet environment as is possible,
- to educate pupils to be aware of, and respond responsibly, to any risks,
- to encourage and support parents, staff and other stakeholders in protecting and educating pupils on how to stay safe online and in the wider world.

3. Roles and Responsibilities

Online safety is a whole-school responsibility dependent on all stakeholders eg staff, governors, advisers, parents and, where appropriate, pupils themselves taking responsibility for the use of the Internet and other forms of communication. Of major importance in creating a safe online learning environment is the internet safety education which occurs in the classroom itself, initiated by the teacher or teaching assistant. Pupils are taught safe and responsible behaviours, and are enabled to develop the critical thinking skills to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. Whilst the Head of School has overall responsibility for safeguarding, which includes online safety issues, a senior teacher has delegated responsibility as the Online Safety Coordinator responsible for online safety management (currently the Deputy Designated Safeguarding Lead).

The Online Safety Council, a group of pupils representing Y1 to Y4, are part of the review process of online safety within school, and help to deliver key online safety message to pupils and parents. The Online Safety Governor meets with the Online Safety Coordinator and then reports regularly to the main governing body.

All members of the school community have core responsibilities within and outside the school environment to:

- use technology responsibly
- accept responsibility for their use of technology
- model best practice when using technology
- report any untoward incidents to the Online Safety Coordinator using the school procedures
- understand that network activity and online communications are monitored, including any personal and private communications made via the school networks.

3.1 Online Safety Coordinator Role and Responsibilities

Our Online Safety Coordinator is the person responsible to the Head of School and governors for the day to day issues relating to Online Safety. The Online Safety Coordinator:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- provides training and advice for staff
- liaises with the Local Authority and other external agencies as relevant
- liaises with school ICT technical staff
- receives reports of online safety incidents and creates logs of incidents to inform future online safety developments
- reviews regularly the output from forensic monitoring software and initiates action where necessary, keeping a log of checks made
- meets termly with the Online Safety Council to discuss current issues and review incident logs
- attends relevant meetings and committees of the Governing Body
- reports regularly to the Senior Leadership Team
- receives appropriate training and support to fulfil their role effectively

3.2 Governors Responsibilities

Governors are responsible for the approval of this policy and for reviewing its effectiveness. A member of the governing body has taken on the role of online safety governor which involves:

- Termly meetings with the Online Safety Coordinator with an agenda based on:
    - monitoring of online safety incident logs
    - reporting to relevant Governors committee / meeting
    - reviewing policy

3.3 Headteacher responsibilities

- The Headteacher is responsible for ensuring the safety (including online safety) of all members of the school community, though the day to day responsibility for online safety is delegated to the Online Safety Coordinator
- The Headteacher and another member of the senior management team will be familiar with the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, including non-teaching staff. (See flow chart on dealing with online safety incidents and other relevant disciplinary procedures)
- The Headteacher is responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

3.4 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 the proper channels: **this duty is on the individual, not the organisation or the school**.
- have an up to date awareness of online safety matters and of the current school online safety policy and practices
- have read, understood and signed the school's Acceptable Use Agreement for staff (including the use of Facebook and other social networking sites)
- report any suspected misuse or problems to the Online Safety Coordinator
- undertake any digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) in a fully professional manner and only using official school systems
- embed online safety issues within the curriculum and other school activities; using the school's progression of skills document as a starting point and reflecting on the needs of the children they are working with
- support all children to develop an understanding of how to keep themselves safe online
- monitor the use of all digital devices and online activity within the classroom / learning space and implement school policies with regard to this

3.5 Responsibilities: ICT Technician

Crabbs Cross Academy employs the services of Lourdes**,** who are aware of online safety best practice, to manage their network and ICT systems.

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 online safety technical requirements (and any relevant Local Authority Online 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 online security policy
- shortcomings in the infrastructure are reported to the ICT coordinator or Head teacher so that appropriate action may be taken.

4. Policy Development, Monitoring and Review

This Online Safety policy has been developed from a template provided by Worcestershire School Improvement Service and through consultation with:

- School Online Safety Coordinator
- Executive Head and Headteacher
- Teachers
- Support Staff
- ICT Technical Staff
- Online Safety Governor
- Parents and Carers
- Pupils

4.1 Schedule for development / monitoring / review of this policy:

This Online Safety policy was approved by the Head teacher on:	
The implementation of this Online Safety policy will be monitored by the:	Online Safety Governor and Online Safety Council under the direction of the Online Safety Coordinator.
Monitoring will take place at regular intervals:	Termly
The Online Safety policy will be reviewed annually (or more regularly in light of any significant new developments). The next anticipated review date will be:	September 2021
Should serious Online Safety incidents take place, the following external persons/agencies should be informed:	Worcestershire Safeguarding Children Board Online Safety Representative Local Authority Designated Officer Worcestershire Senior Advisor for Safeguarding Children in Education West Mercia Police

5. Network security and monitoring

The school reviews both physical and network security regularly and monitors who has access to the system, consulting with the LA where appropriate:

- Anti-virus software is installed on all computers and updated regularly.
- Central filtering is provided and managed by IBS Schools.
- All staff are made aware that if an inappropriate site is discovered it must be reported to the Online Safety Coordinator who will report it to the IBS Schools Service Desk to be blocked.
- Pupils are taught to tell an adult immediately if they open a site which has unpleasant content or which worries them.
- All incidents will be recorded in the Online Safety log, kept by the Online Safety Coordinator, for audit purposes.
- Requests for changes to the filtering will be directed to the Online Safety coordinator in the first instance, who will forward these on to IBS Schools or liaise with the Head teacher as appropriate.
- The school uses Policy Central on all school owned equipment to ensure compliance with the Acceptable Use Agreements. This is monitored by the Online Safety Coordinator and another nominated member of staff, regularly, (LB) in liaison with the Head teacher.

5.1 Filtering

The school has a managed filtering service in place which filters internet content and provides an important means of preventing users from accessing material that is illegal or inappropriate in an education context. The filtering system cannot, however, provide a 100% guarantee that it will do so. There is some flexibility to allow the school to modify the filter.

The day to day responsibility for the management of the school's filtering policy is held by the Online Safety Coordinator (with ultimate responsibility resting with the Headteacher and Governors). Logs of changes to and breaches of the filtering system will be kept by the Online Safety Coordinator.

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

- Be logged in change control logs
- Be reported to a second responsible person (Head teacher / Computing Coordinator)
- Be reported to and authorised by, a second responsible person prior to changes being made (this will normally be the class teacher who originally made the request for the change)

All users have a responsibility to report immediately to class teachers / Online 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 programs or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

5.2 Passwords

- All staff are issued with their own username and password for network access.
- Supply staff are issued with the temporary 'Supply' ID.
- Where pupils have personal logins they are taught not to share them; however it is acknowledged that when pupils work together on a computer one or the other will need to login. (see below for Acceptable Use protocols)
- Passwords for servers are encrypted to ensure they are secure. These passwords are available to the School Business Manager and Computing Lead, and to the Head in case of need.
- The school's Online Safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of school.

5.3 Mobile technologies (see also Section 8)

Laptops and iPads are provided for teachers for educational purposes and their own professional development. These can be used outside of school, although staff are advised to ensure these are kept safe and secure at all times e.g. they should not be left locked in the boot of a car as this is not covered by insurance. The online safety policy and user agreements also apply to laptops and iPads at all times. No non-educational software should be installed on these. Any laptops or other storage devices that are used by staff and which are not encrypted, should not contain any personal data relating to pupils.

5.4 Online learning technologies

The school subscribes to the accredited County Council Broadband service as its ISP (Internet Service Provider) which provides an effective and safe online learning environment including Internet access, e-mail service and school website hosting. To safeguard against risks and unacceptable materials and activities these services include filtering and content control, firewall and virus protection, and software for monitoring access to the Internet by each individual log-in. Any new technologies will only be made accessible to the school community when they have been assessed for their nature, content, educational benefit, safety and security. Safe disposal of any computing equipment is the responsibility of the Online Safety Coordinator under the advice of the ICT Technician.

6. Online Safety Awareness and training

Online safety awareness and education is an essential part of the school's online safety provision. To achieve this, the school:

- provides a specific program of online safety learning as part of ICT / PSHE, and reinforces key online safety messages throughout the school curriculum
- makes this policy, and related documents, available on the school website for everyone to access
- updates and reviews this policy, and related documents, with staff and governors on an annual basis
- displays relevant online safety information in all classrooms and other areas where computers are used
- ensures learning technologies are reviewed by relevant coordinators and their purpose
- considers online safety ideas for their use and disseminated through curriculum meetings / staff meetings / training sessions
- parents are provided with online safety advice and guidance on the school website, and when appropriate via newsletters or parents' meetings / workshops.

6.1 Acceptable Use of the Internet

The Internet can provide pupils and all stakeholders with opportunities to experience and use a wide range of activities, resources, and information to support and enhance the learning and teaching across the whole school curriculum.

- All pupils will be expected to access the Internet unless parents have indicated otherwise at the time their child is admitted to school.
- Adults in school who use online technologies are asked to read, sign and comply with the relevant Online safety Acceptable Use Agreement.
- Parents are asked to discuss with their children the Online safety Acceptable Use Agreement for pupils appropriate to the key stage their child is in, and sign the agreement.
- In the Early Years Foundation Stage access to the Internet is with the teacher or teaching assistant as a collaborative introduction to websites. Where children are working independently, they are closely supervised to ensure that they are only using activities set up by teaching staff.
- In KS1 the majority of access to the Internet will be by the teacher, by adult demonstration or through carefully supervised access to specific approved online materials.
- In KS2 internet access will form part of delivery of the curriculum and to encourage independent research and learning.
- Pupils will only access and use the Internet when a suitable adult, who has signed their agreement to the policy, is present in the room.
- Pupils will be taught how to use the internet safely and responsibly as an integral part of online learning across the curriculum and supported by the school's online safety program.
- Pupils will be taught how to be safe while online at home, as well as at school.

Videos from 'YouTube' which are to be used to support and enhance learning and teaching are vetted prior to use with children. Such videos are NOT to be accessed or loaded whilst children are present so must be loaded on full screen prior to children coming into the classroom / hall. Alternatively, when possible the YouTube downloader should be used, depending on the settings of a video itself working within this.

6.2 Email

The Internet as a means to contact people and organisations is an extremely valuable tool, encouraging the development of communication skills and transforming the learning process by opening up extra possibilities. However, just as in the real world, children may get involved in inappropriate, antisocial or illegal behaviour while using new technologies eg, cyberbullying, identity theft, and arranging to meet people they have met online. The e-mail system is regularly monitored and should not be considered private communication.

6.3 Staff

All staff are given a school e-mail address and it is expected that this should be used for all professional communication. This is to ensure safeguarding for all adults. Staff are allowed to access personal e-mail accounts on the school system outside directed time and are advised that any messages sent using the school equipment must be in line with the school's e-mail policy. In addition, they are also advised that these messages will be scanned by the monitoring software.

7. Online Safety Training

7.1 Staff

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

- A planned program of formal online safety training will be made available to staff. An audit of the online safety training needs of all staff will be carried out regularly.
- It is expected that staff will identify any individual online safety training needs where they feel they have any gaps in their knowledge. This should be brought to the attention of the Online Safety Coordinator.
- All new staff should receive online safety training as part of their induction program, ensuring that they fully understand the school online safety policy and acceptable use agreements which are signed as part of their induction
- The Online Safety Coordinator will be CEOP trained.
- The Online Safety Coordinator will receive regular updates through attendance at local authority or other training sessions and by reviewing guidance documents released by the DfE, the local authority, the WSCB and others.
- All teaching staff have been involved in the creation of this online safety policy and are therefore aware of its content
- The Online 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, is sought from Worcestershire School Improvement Learning Technologies Team when appropriate

7.2 Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee or group involved in ICT, online 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 online safety governor works closely with the online safety coordinator and reports back to the full governing body.

7.3 Parent and Carer Awareness raising

Many parents and carers have only a limited understanding of online 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 online experiences. Parents 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 parents and carers through:

- *Letters, newsletters, website*
- *Parents evenings*

- *Reference to the parents materials on the Worcestershire 'Stay Safe Online' web page (http://www.worcestershire.gov.uk/info/20329/protection_from_harm/1681/stay_safe_online)*

7.4 Pupils

Whilst children will, at times, use emails as part of their learning across the curriculum, the school does not use chat rooms or instant messaging. Children will however be made aware of the risks involved in all of these and ways of avoiding them, as part of their online safety and digital literacy skills development. Pupils may have access to class based e-mail accounts as part of learning and teaching. These are accessed in the presence of, and monitored by, the class teacher, where safe practise will be discussed and modelled. Any inappropriate emails must be reported to the Online Safety coordinator / class teacher as soon as possible.

If any staff believe that a child has been targeted with e-mail messages by parties with criminal intent, the messages will be retained, the incident recorded, and the Governors and the child's parents informed. Advice will also be taken regarding possible further steps, including investigation using forensic monitoring software.

To provide an email environment for pupils which is as safe and secure as possible the school has adopted the following practice:

- the use of the e-mail program within Purple Mash to enable children to practice sending and receiving emails safely;
- steps are taken to verify the identity of any school or child seeking to establish regular e-mail with this school;
- pupils read e-mail messages when a member of staff is present, or the messages have been previewed by the teacher;
- children are taught not to open or respond to emails from a previously unknown source, but to tell the member of staff present in the room so that appropriate action can be taken.
- pupils save their emails/messages to draft for the teacher or teaching assistant to approve before being sent (as they would with a conventional letter) OR, if using Purple Mash, teachers are sent all emails to authorise before being sent.

7.5 Online 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 online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online 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.

Online Safety education will be provided in the following ways:

- Regular online safety sessions are planned as part of ICT, PSHE and other lessons. These key learning messages are regularly revisited, covering the use of ICT and new technologies both in school and outside school.
- Key online 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 the need for the pupil Acceptable Use Agreements (see appendices 1-4).
- Pupils will be encouraged 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.
- 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 children 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.

7.6 Information Literacy

- Pupils should be taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information by employing techniques such as:
    - ✓ 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 guide for our online safety provision* https://www.thinkuknow.co.uk/

8. Use of other communication and mobile technologies

8.1 Mobile phones

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:
    - ✓ Personal hand held devices 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.
    - ✓ Mobile phones or hand-held personal devices are not to be used to take photographs or videos of pupils under any circumstances.

Pupils are not allowed to bring mobile phones into school. The Educations and Inspections Act 2006 grants the Head the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Head will exercise this right at their discretion.

The school internet / email facilities should be used only for educational purposes during teaching and learning time. Staff are advised not to, but if they do choose to use school internet facilities for personal purposes, such as online banking or purchasing of items for personal use, this will be at their own risk.

Staff are advised not to give out their personal mobile telephone numbers to parents, even when travelling on a school trip. The school has its own mobile phone which is to be used by staff during trips and visits.

8.2 Emails

Access to email is provided for all users in school via Microsoft 365 (Outlook) using individual IDs.

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 for school / work purposes and not for personal use
- Users need to be aware that email communications are 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 need to be aware that any personal emails will be monitored by the school Forensic Monitoring Software and should not use personal emails to share / exchange any sensitive or personal data relating to pupils (or any other sensitive matters).
- Personal e-mails may only be accessed outside of teaching and learning times.
- Users must immediately report to their class teacher / Online Safety Coordinator 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.

8.3 Use of Internet networking sites eg Facebook

Staff are reminded about the use of internet sites such as Facebook. It is recognised that there is a need for discretion when using such sites. If staff use social networking sites eg. Facebook / Instagram, no reference is to be made to Crabbs Cross Academy by name, nor by description of events, comments, people, or feelings towards the school or any other schools in the Trust.

It is neither professional nor appropriate to allow parents, students or ex-students onto your Facebook page. Staff should be mindful that anything that can be seen by the public may reflect on the school (this includes photographs).

All staff are required to sign the Acceptable Use Agreement in relation to social networking sites (see Appendices).

9. Publishing of Content via digital resources or the Internet

It is recognised that staff and children may at some time produce and publish materials on an Internet website associated with the School such as the school website.
The school has its own website hosted through its recognised reputable ISP. Materials produced as part of children's learning may be published on it unless parents have indicated otherwise at the time their child is admitted to school. Pupils' full names will not be published outside the school environment. Should anyone wish to contact the school in response to such materials they are advised to contact the school via the school office by email or telephone.

No materials will be published on the Internet which contains any unacceptable images, language or content.

Parents are advised that they may take photographs or videos of children's performances only for personal use. These must not be published on the internet eg on Facebook or Instagram.

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.

Pupils must not take, use, share, publish or distribute images of others without their permission.

Infringement of these rules will be taken as a serious disciplinary issue.

9.1 Copyright Issues

It is recognised that all materials on the Internet are copyright, unless copyright is specifically waived. It is the school's policy that the copyright of Internet materials will be respected. Where materials are published on the Internet as part of the teacher's professional duties, copyright will remain with the County Council. Internet published materials will contain due copyright acknowledgements for any third party materials contained within them. Staff are provided with guidance on using advanced search engine settings which can filter results according to copyright.

9.2 Use of the school's Internet facility by visitors and guests

Members of school staff are expected to take responsibility for the actions of any adult guests or visitors who they allow or encourage to use the school Internet facilities. The essential "dos and don'ts" are explained to such visitors and guests prior to their use of the Internet.
Unacceptable use will lead to the immediate withdrawal of permission to use the school Internet facility.
A Guest login for the network is available for use by supply teachers. A log is kept of supply teachers using these.

10. Responding to incidents of inappropriate or undesirable use

10.1 Unintentional exposure of children to inappropriate content

It is the school's policy that every reasonable step should be taken to prevent exposure of children to undesirable materials on the Internet. It is recognised that this can happen not only through deliberate searching for such materials, but also unintentionally when a justifiable Internet search yields unexpected results.
If any users discover undesirable sites, the URL (web address) and content must be reported to the Online Safety Coordinator who will inform the ISP as soon as possible.

10.2 Intentional access of undesirable content by children

Children should never intentionally seek offensive material on the Internet. In any such incident the matter will be treated as a disciplinary matter, and the parents of a child or children will be informed.

In the event of children being exposed to undesirable materials, however accessed, the following steps will be taken:

- pupils will notify a teacher or teaching assistant immediately
- initially the Online Safety Coordinator will be notified by the teacher, and then the Head of School
- the incident will be recorded in a central log, held by the Online Safety Coordinator; the frequency and nature of incidents will be monitored and reported to Governors
- the County approved forensic monitoring software will be used to investigate as appropriate
- parents will be notified at the discretion of the Head teacher according to the degree of seriousness of the incident (for example, exposure to materials that include common profanities might not be notified to parents, but exposure to materials that included pornographic images would be notified)

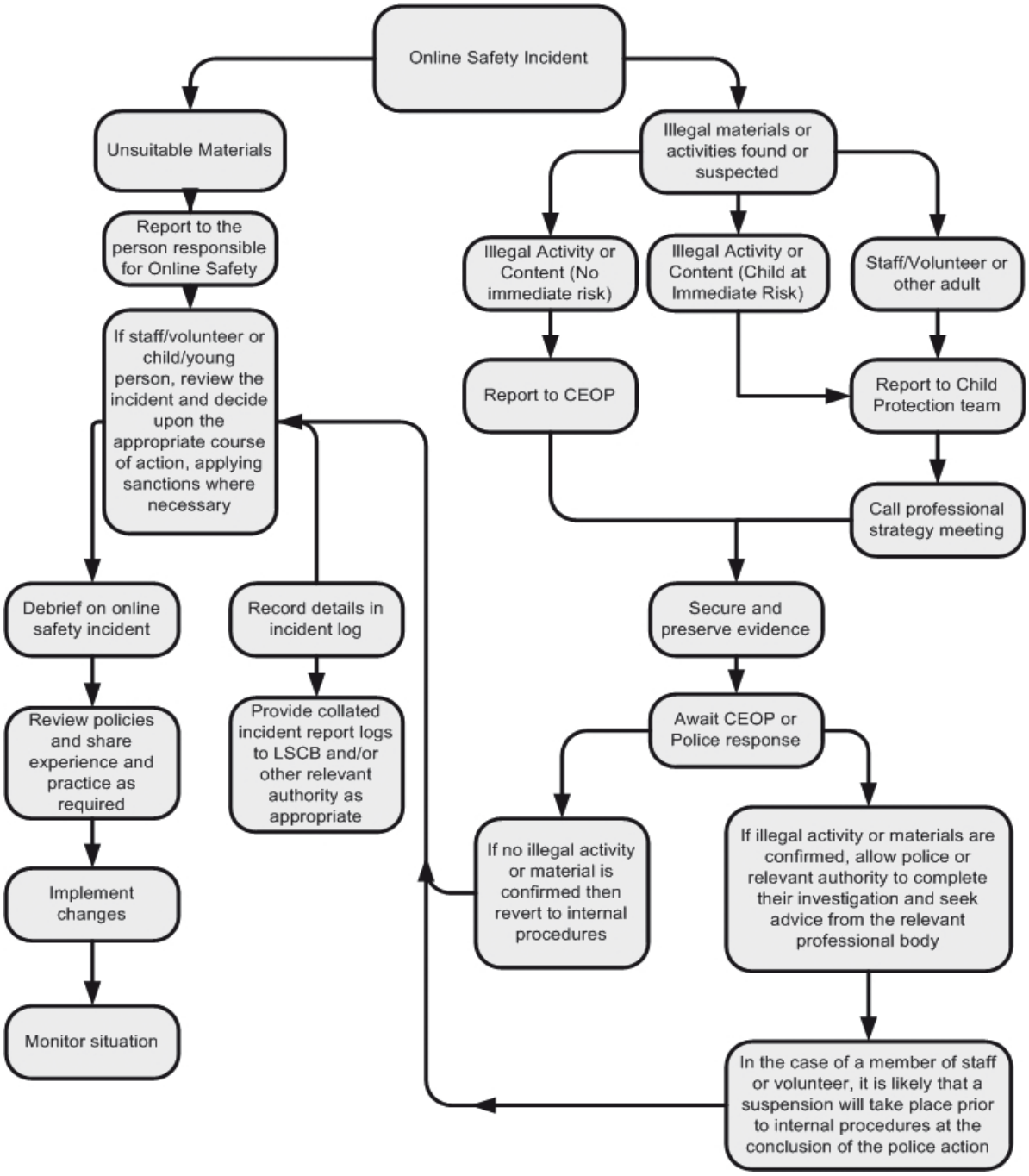
10.3 Intentional access to undesirable content by adults

Deliberate access to undesirable materials by adults is unacceptable, and will be treated as a disciplinary issue. If abuse is found to be repeated, flagrant or habitual, the matter will be treated as a very serious disciplinary issue. The Governors will be advised and the LA will be consulted. The County Council guidance regarding what to do with computers which have been used inappropriately will be followed in cases of serious misuse.

10.4 Reporting of online 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:



11. Disposal of ICT equipment

Will conform to:
The Waste Electrical and Electronic Equipment Regulations 2006
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

Appendix 1

Crabbs Cross Academy

Acceptable Use Agreement - for learners in Reception and KS1

I want to feel safe all the time.

I agree that I will:

To keep myself and others safe:

* Tell an adult if I see something that upsets me on the screen
* Ask an adult to help me if I'm not sure what to do or if something goes wrong.
* Always keep my passwords a secret
* Not tell people about myself online (I will not tell them my name, my school, anything about my home, family or pets)
* Never agree to meet a stranger
* Make sure all the messages I send are friendly
* Only use activities which my teacher has said are ok
* Take care of the computers

I know that if I break the rules, I might not be allowed to use the computing equipment in school.

My name	
My class	
Signed (Child if in Year 2)	
Signed (Parent if the child is in Reception or Year 1)	
Date	

Appendix 2

Acceptable Use Agreement – Letter for parents of Reception and Key Stage 1

Dear Parent/Carer,

Please find attached our Acceptable Use Agreement for Reception and Key Stage 1 children.
At Crabbs Cross Academy, we take the safety of your child very seriously and this includes keeping them safe online. The Acceptable Use Agreement are set and agreed by the staff and governors at the school in order to keep your child safe on the internet at all times.

Please be aware that the curriculum which the children follow in the Foundation Stage and Key Stage One is different and therefore the above points will not be relevant for all children at all times. They will become relevant over time and children will agree to follow them as and when they meet them within their computing learning.

We would be very grateful, therefore, if you would discuss the contents of the agreement with your child and, if they are in Year 2 to sign the Agreement and return it to the School Office. If your child is in Reception or Year 1, please ensure that you have discussed the Agreement with your child and that they understand the rules, then sign and return the Agreement yourself.

We would also be grateful, if you would please read and sign the Parental Agreement below and return it with the Acceptable Use Agreement.

Thank you in advance for your continuing support with this very important matter.

Please return cut off slip to school

Crabbs Cross Academy
Acceptable Use Agreement
for learners in Reception and Key Stage 1

Name of Child: _____ Class: _____

I/we have read, understand and will comply with the Acceptable Use Agreement and guidelines for Crabbs Cross Academy and hereby give our permission for our child to participate in school internet and other computer based activities and to be monitored whilst doing so. We agree that our child will follow the rules set out in the Acceptable Use Agreement, which will be regularly shared with them at school.

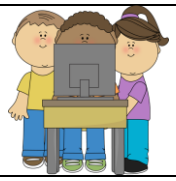
Parent / Carer Signature: _____ Date: _____

Appendix 3

Crabbs Cross Academy

Acceptable Use Agreement - for learners in KS2

I understand that while I am a member of Crabbs Cross Academy I must use technology in a responsible way.

	**For my own personal safety:** * I understand that my use of technology (especially when I use the internet) 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 programs of any type on the devices belonging to the school without permission.

I understand that I am responsible for my actions and the consequences. I know that if I break the rules, I might not be allowed to use the computing equipment in school.
I have read and understood the above and agree to follow these guidelines:

Name:	
Signed:	
Date:	

Appendix 4

Acceptable Use Agreement - Letter for parents of Key Stage 2

Dear Parent/Carer,

Please find attached our Acceptable Use Agreement for Key Stage 2 children.

At Crabbs Cross Academy, we take the safety of your child very seriously and this includes keeping them safe online. The Acceptable Use Agreement are set and agreed by the staff and governors at the school in order to keep your child safe on the internet at all times.

Throughout Key Stage 2, your child will be taught about safe internet and technology use as part of our Computing Curriculum and these rules will be explored in greater depth. In the meantime, we would be very grateful, therefore, if you would discuss the contents of the agreement with your child and sign the Agreement and return it to the School Office. Please ensure that you have discussed the Agreement with your child and that they understand the rules, then sign and return the Agreement yourself.

We would also be grateful, if you would please read and sign the Parental Agreement below and return it with the Acceptable Use Agreement.

Thank you in advance for your continuing support with this very important matter.

Please return cut off slip to school

Crabbs Cross Academy
Acceptable Use Agreement
for learners in KS2

Name of Child: _____ Class: _____

I/we have read, understand and will comply with the Acceptable Use Agreement and guidelines for Crabbs Cross Academy and hereby give our permission for our child to participate in school internet and other computer based activities and to be monitored whilst doing so. We agree that our child will follow the rules set out in the Acceptable Use Agreement, which will be shared with them regularly at school.

Parent / Carer Signature: _____ Date: _____

Appendix 5

Crabbs Cross Academy

Acceptable Use Agreement for Staff and Volunteers

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 online 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, using Forensic Monitoring Software.
- 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 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 by the school 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'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.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

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

- If I am required to work from home, where possible I will use a school/trust device. If I do not have access to a school/trust device, in agreement with the headteacher or CEO, I will only use my personal devices for homeworking as agreed in the online safety policy 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 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.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist 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 GDPR Policy. Where personal data is transferred outside the secure school network, it must be kept secure at all times.
- 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 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 school, but also applies to my use of school ICT systems and equipment out of school and to my use of personal equipment in 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 Safeguarding Body and in the event of illegal activities the involvement of the police.

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

Staff / volunteer Name:	
Signed:	
Date:	

Appendix 6

Crabbs Cross Academy

Acceptable Use Agreement for Teachers regarding the use of Facebook or other similar Social Networking sites.

This Agreement is in line with Teachers' Professional Standards and the Endeavour Schools Trust expectations for all employees.
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. You may consider using a profile name that is not the name you use at work; for example a maiden name or your first and middle name instead of surname.
- 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, 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'. Where members of staff are parents of children within the school, they should avoid accepting other parents as friends where possible.
- Do not use Facebook 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, inform your head teacher. 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_____ Signed_____

Appendix 7 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 template for recording the review of potentially harmful websites can be found at the following webpage: https://swgfl.org.uk/online-safety-policy-templates-for-schools/

Appendix 8 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 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 9 Supporting resources and links

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

General

South West Grid for Learning - https://swgfl.org.uk/online-safety/

Child Exploitation and Online Protection Centre (CEOP) - http://www.ceop.gov.uk/

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

ChildNet - https://www.childnet.com/

InSafe - http://www.saferinternet.org/ww/en/pub/insafe/index.htm

Byron Reviews ("Safer Children in a Digital World") - http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews

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

London Grid for Learning - https://www.lgfl.net/online-safety/#

National Education Network - https://www.nen.gov.uk/advice-for-schools/online-safety/

National Online Safety - https://nationalonlinesafety.com/

WMNet – http://www.wmnet.org.uk

Cyber Bullying

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

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

Social networking

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

Links to other resource providers

BBC Webwise - http://www.bbc.co.uk/webwise/topics/using-the-web/

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

DfE Guidance 'Teaching online safety in school' - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf

Appendix 10 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 schools provided by NAACE for DfE
INSET	In-service Education and Training
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
LSCB	Local Safeguarding Children Board
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (eg WMNet) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
SRF	Self Review Framework – a tool maintained by Naace used by schools 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 schools in the region and connects them all to the National Education Network (Internet)
WSCB	Worcestershire Safeguarding Children Board (the local safeguarding board)