E-Safety Policy

Rushwick CE Primary School

This policy is based on a template from the South West Grid for Learning (SWGL), an advised policy for Worcestershire schools.

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-safeguarding policy has been written from a template provided by Worcestershire School Improvement team which has itself been derived from that provided by the South West Grid for Learning.

The ICT coordinator, under the direction of the head teacher and SLT, is also responsible for overseeing e-safety in the following ways:

- Establishing and reviewing the school e-safety policies / documents.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident.
- Facilitating training and advice for staff.
- Liaising with school peripatetic support.

- Receiving reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meeting with e-safety governor to discuss current issues and review incident.
- Attending relevant meetings and committees of Governing Body.
- Reporting regularly to Senior Leadership Team.
- Receiving appropriate training and support to fulfil their role effectively.

Governors

Governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors (or a governors' committee) receiving regular information about e-safety incidents and monitoring reports.

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 another member of the senior management team 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.

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.
- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood and signed the 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) in a fully professional manner and only using official school systems.
- They embed e-safety issues in the curriculum and other school activities, also acknowledging the planned e-safety curriculum programme of study.

ICT Support

The peripatetic 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.
- 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 coordinator or head teacher so that appropriate action may be taken.

Policy review

Monitoring will take place at regular intervals, annually or as issues occur e.g. 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.
- Worcestershire Senior Adviser for Safeguarding Children in Education.
- West Mercia Police.

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.

Head teachers are empowered, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place 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 e-safety behaviour that take place out of school.

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 encouraged to sign before being given access to school systems.

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

- Pupils (EYFS + KS1 / KS2).
- Staff (and volunteers).
- Parents / carers.
- Community users of the school's ICT system.

Acceptable Use Agreements are introduced at parents' induction meetings and signed by all children as they enter school (with parents possibly signing on behalf of children below Year 2). Children are encouraged to re-sign on entering KS2.

All employees of the school and volunteers 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.

Whole School approach and links to other policies

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

- Curriculum Policies.
- Safeguarding and Child Protection.
- Behaviour and Anti-Bullying.

- Home-School Agreement.
- School systems and Data Security Policy.
- ICT progressions.
- Use of images.

Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context (those in ***bold italics*** are illegal) and that users should not engage in these activities when using school equipment or systems (in or out of school).

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

- ***Child sexual abuse images***.
- ***Grooming, incitement, arrangement or facilitation of sexual acts against children.***
- ***Possession of extreme pornographic images.***
- ***Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation).***
- *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:

- 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).
- On-line gambling and non-educational gaming.
- 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.

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.

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:

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:

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.

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

Pupils are not currently permitted to bring their personal hand held devices into school.

Email:

Access to email is provided for all users in school using their Global IDs. In addition, messaging (and email for staff) is available through the school's learning platforms.

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.
- Users must immediately report to their class teacher / e-safety coordinator – in accordance with the school 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
- Use of personal email accounts in school / on school network is not permitted without permission of Headteacher / Deputy Headteacher.

Videoconferencing:

- Desktop video conferencing and messaging systems linked to school Broadband is the preferred communication option in order to secure a quality of service that meets school curriculum.
- Permission for children to take part in video conferences is sought from parents / carers at the beginning of the pupil's time in school. Only where permission is granted may children participate.

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. 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 approved 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

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 a pupil's first name will be used on the website, and only then when necessary.
- Detailed calendars will not be published on the school website, though a basic calendar of events for parents and Ofsted will be published.
- 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:
    - *Where possible, photographs will not allow individuals to be recognised.*
    - *Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.*
    - *A Pupil's work can only be published with the permission of the pupil and parents or carers.*

Learning Platform:

- Class teachers monitor the use of the learning platform by pupils regularly during all supervised sessions, but with particular regard to messaging and communication.
- Staff use is monitored by the super-user/administrator.
- User accounts and access rights can only be created by the school administrator.
- Pupils are advised on acceptable conduct and use when using the learning platform.
- Only members of the current pupil, parent/carers and staff community will have access to the learning platform.
- When staff, pupils, etc leave the school their account or rights to specific school areas will be disabled (or transferred to their new establishment if possible / appropriate).
- Any concerns with content may be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- The material will be removed by the site administrator if the user does not comply.
- Access to the learning platform may be suspended for the user.
- The user will need to discuss the issues with a member of SLT before reinstatement.
- A pupil's parent/carer may be informed.

Professional standards for staff communication

In all aspects of their work in our school, teachers abide by the broad Professional Standards for Teachers.

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 also inform this process.

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.

Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school remains vigilant over the associated risks and provides preventative measures which are relevant to the situation in this school. Pupils are made aware of the importance of filtering systems through the school's e-safety education programme.

As a school buying broadband services from Worcestershire County Council approved partner, we automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

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

- Signing the Acceptable Use Agreement.
- Briefing in staff meetings, training days, memos etc. (timely and ongoing).

Parents will be informed through the Acceptable Use Agreement and publishing of this policies on the school website.

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 school e-safety coordinator.
- The e-safety coordinator checks the website content to ensure that it is appropriate for use in school.

THEN

- If agreement is reached, the e-safety coordinator makes a request to the Broadband Team.
- 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.

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.

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.

This is dealt with in detail in IBS / CAPITA School's System and Data Security advice. Please see that document for more information.

Teachers frequently discuss issues relating to data security and how it relates to staying safe in and out of school.

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

- A planned e-safety programme is provided as part of Computing, PHSE and other lessons. 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 the need for the pupil Acceptable Use Agreement and 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.

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.
- 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

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 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.

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

- Letters, newsletters, web site, learning platform.
- Parents' evenings.

Date of Policy: *September 2020*

Policy Review: *September 2022*

Rushwick School Acceptable use policy 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 the school's work.

Child's name:

Parent's name

Parent's 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 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 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

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 to record evidence of activities in lessons and out of 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.

As the parent / carer of the above pupil, I agree to the school taking and using digital images of my child(ren). I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at school events which include images of children, I will abide by these guidelines in my use of these images.

Parent's signature:

Date:

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 school website and in the school's learning platform.

As the parent / carer of the above child I give my permission for this activity.

Parent's signature:

Date:

Permission for my child to participate in video-conferencing

Videoconferencing technology is used by the school in a range of ways to enhance learning – for example, by linking to an external "expert", or to an overseas partner school. Video conferencing only takes place under teacher-supervision. Independent pupil use of video-conferencing is not allowed.

As the parent / carer of the above child I give my permission for this activity.

Parent's signature:

Date:

The school's e-safety Policy, which contains this Acceptable Use Agreement, and the one signed by your child (to which this agreement refers), is available on the school website.

Acceptable use policy 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 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 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 school) within these guidelines. I understand that failure to comply with this agreement will result in my access to the school's 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:

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.

Sample documents for recording the review of and action arriving from the review of potentially harmful websites can be found in the PDF version of the SWGfL template e-safety policy (pages 36-38):
http://www.swgfl.org.uk/Files/Documents/esp_template_pdf

Supporting resources and links

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

- South West Grid for Learning "SWGfL Safe" - http://www.swgfl.org.uk/Staying-Safe
- Child Exploitation and Online Protection Centre (CEOP) http://www.ceop.gov.uk/
- ThinkUKnow http://www.thinkuknow.co.uk/
- ChildNet http://www.childnet-int.org/
- 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 - http://www.lgfl.net/esafety/Pages/education.aspx?click-source=nav-esafety
- Kent NGfL http://www.kented.org.uk/ngfl/ict/safety.htm
- Northern Grid - http://www.northerngrid.org/index.php/resources/e-safety
- National Education Network NEN E-Safety Audit Tool - http://www.nen.gov.uk/hot_topic/13/nen-e-safety-audit-tool.html
- WMNet – http://www.wmnet.org.uk
- WES Worcestershire E-Safety Site – http://www.wes.networcs.net
- EU kids Online http://www2.lse.ac.uk/media@lse/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/behaviour/tacklingbullying/cyberbullying/
- Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm
- Cyberbullying.org - http://www.cyberbullying.org/
- East Sussex Council - Cyberbullying - A Guide for Schools:
- https://czone.eastsussex.gov.uk/supportingchildren/healthwelfare/bullying/Pages/eastsussexandnationalguidance.aspx
- CyberMentors: young people helping and supporting each other online - http://www.cybermentors.org.uk/

Social networking

- Digizen – "Young People and Social Networking Services": http://www.digizen.org.uk/socialnetworking/
- Ofcom Report: Engaging with Social Networking sites (Executive Summary)
- http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/
- Connect Safely - Smart socialising: http://www.blogsafety.com

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 schools" 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
- See also Becta (archived) resources above
- Parents' guide to new technologies and social networking
- http://www.iab.ie/

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 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/
- NCH - http://www.stoptextbully.com/
- Chatdanger - http://www.chatdanger.com/
- Internet Watch Foundation: http://www.iwf.org.uk/media/literature.htm
- Digizen – cyber-bullying films: http://www.digizen.org/cyberbullying/film.aspx
- London Grid for Learning: http://www.lgfl.net/esafety/Pages/safeguarding.aspx?click-source=nav-toplevel

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

Rushwick Primary School

Acceptable Use Agreement

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 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 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 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.
- 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 (see **Capita and Data Security advice**).
- 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 School Personal Data documentation (see e-safety policy). 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 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 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:	