Rakegate Primary School

E-safety Policy

Development / Monitoring / Review of this Policy

This E-safety policy has been developed by a working group made up of:

- *The Head teacher*
- *E-Safety Officer*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Governors*
- *Parents and Carers*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Governing Body*	
The implementation of this e-safety policy will be monitored by the:	*E-Safety Coordinator* *Senior Leadership Team*
Monitoring will take place at regular intervals:	Yearly
The *Board of Directors / Governing Body / Governors Sub Committee* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Termly
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*January 2019*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Mrs Ashton-Jones Link Governor for safeguarding

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Monitoring logs of internet activity (including sites visited)*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of*
  - *students / pupils*
  - parents / carers
  - *staff*

Context and Background

The technologies
ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information.

Current and emerging Internet and online technologies used in school and more importantly in many cases, used outside of school by children include:

- The Internet – World Wide Web
- E-mail
- Instant messaging (often using simple web cams) e.g. Instant Messenger)
- Web based voice and video calling (e.g. Skype)
- Online chat rooms
- Online discussion forums
- Social networking sites (e.g. Facebook)
- Blogs and Micro-blogs (e.g. Twitter)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites (e.g. You Tube)
- Music and video downloading (e.g. iTunes)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging and internet access

Our whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools.
- Policies and procedures, with clear roles and responsibilities.
- E-Safety teaching is embedded into the school curriculum and schemes of work.

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the *school.*

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about e-safety incidents and monitoring reports. A member of the *Governing Body* has taken on the role of Child Protection/ Safeguarding Officer and this will encompass the role of the *E-Safety Governor.*

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

- *regular meetings with the E-Safety Co-ordinator*
- *regular monitoring of e-safety incident logs*
- *regular monitoring of filtering / change control logs*
- *reporting to relevant Governors meeting*

Headteacher and Senior Leaders:

- **The *Headteacher* has a duty of care for ensuring the safety (including e-safety) of members of the school community**, though the day to day responsibility for e-safety will be delegated to the *E-Safety Co-ordinator.*
- **The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.** (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority HR / other relevant body* disciplinary procedures).
- *The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.*
- *The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
- *The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.*

E-Safety Coordinator:

- leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff

- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- meets regularly with E-Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings
- reports regularly to Senior Leadership Team

Technical staff:

The *ICT Technician* is responsible for ensuring:

- **that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the *school* meets required e-safety technical requirements and any *Local Authority / other relevant body* E-Safety Policy / Guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the *network / internet / Virtual Learning Environment / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Headteacher and E-Safety Coordinator* for an investigation and any actions / sanctions to be carried out.
- *that monitoring software / systems are implemented and updated as agreed in school policies*

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- **they have an up to date awareness of e-safety matters and of the current *school* e-safety policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)**
- **they report any suspected misuse or problem to the *Headteacher and E-Safety Coordinator* for an investigation and any actions / sanctions to be carried out.**
- **all digital communications with pupils / parents / carers should be on a professional level** *and only carried out using official school systems*
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- *in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*

Safeguarding Officer

Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from the *school* community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. Depending on the size or structure of the *school* this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the *Governing Body.*

Members of the *E-safety Group* (or other relevant group) will assist the *E-Safety Coordinator (or other relevant person, as above)* with:

- the production / review / monitoring of the school e-safety policy / documents.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Pupils:

- are responsible for using the *school* digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the *school's* E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The *school* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature.* Parents and carers will be encouraged to support the *school* in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events

- access to parents' sections of the website / pupil records

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of *pupils* in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- **A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited**
- **Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities**
- **Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**
- **Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- *Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school*
- *Staff should act as good role models in their use of digital technologies the internet and mobile devices*
- *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.*
- *It is accepted that from time to time, for good educational reasons, **staff** may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*

E-Safety for Pupils

We believe it is our responsibility to prepare pupils for their lives in the modern world, and ICT is an integral part of that world. At our school we are committed to teaching pupils to use the ICT effectively and appropriately in all aspects of their education.

Internet access at school

Use of the Internet by pupils

Internet access is carefully controlled by teachers according to the age and experience of the pupils and the learning objectives being addressed. Pupils are always actively supervised by an adult when using the Internet, and computers with Internet access are carefully located so that screens can be seen at all times by all who pass by.

Access for all pupils

In line with our inclusion policies across the school, we want to ensure that all out pupils have access to the Internet, particularly where this will directly support their learning.

Using the Internet for learning

The Internet is now an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials.

Using the Internet for learning is now a part of the Computing Curriculum (Sept 2014) We teach all of our pupils how to find appropriate information on the Internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

- Teachers carefully plan all Internet-based teaching to ensure that pupils are focussed and using appropriate and relevant materials.
- Children are taught how to use search engines and how to evaluate Internet-based information as part of the ICT curriculum, and in other curriculum areas where necessary.
- They are taught how to recognise the difference between commercial and non-commercial web sites, and how to investigate the possible authors of web-based materials.
- They are taught how to carry out simple checks for bias and misinformation
- They are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.

Teaching safe use of the Internet and ICT

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home and we use the Kidsmart safety code to support our teaching in this area:
Kidsmart has been developed by the Childnet charity, and is endorsed by the DfES
http://www.kidsmart.org.uk

The main aspects of this approach include the following five **SMART** tips:

- **Safe** - Staying safe involves being careful and not giving out your name, address, mobile phone no., school name or password to people online...
- **Meeting** someone you meet in cyberspace can be dangerous. Only do so with your parents'/carers' permission and then when they are present...
- **Accepting** e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages...
- **Remember** someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging end the conversation...

- **Tell** your parent or carer if someone or something makes you feel uncomfortable or worried...

Suitable material

We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

Non-Education materials

We believe it is better to support children in finding their way around the Internet with guidance and positive role modelling rather than restrict Internet use to strict curriculum based research. As well as Internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information. There is a selection of links to such resources available on the school website.

Unsuitable material

Despite the best efforts of the LA and school staff, occasionally pupils may come cross something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.

The action will include:
1. Making a note of the website and any other websites linked to it.
2. Informing the ICT Administrator
3. Logging the incident – Concern Form
4. Discussion with the pupil about the incident, and how to avoid similar experiences in future

Using E-Mail at school

E-Mail is a valuable and stimulating method of communication that plays an important role in many aspects of our lives today. We believe it is important that our pupils understand the role of e-mail, and how to use it appropriately and effectively.

- *We teach the use of e-mail as part of our ICT curriculum, and use appropriate pupil email accounts where necessary.*
- *Pupils are not allowed to access personal e-mail using school Internet facilities.*

Chat, discussion and social networking sites

These forms of electronic communication are used more and more by pupils out of school, and can also contribute to learning across a range of curriculum areas.

Online chat rooms, discussion forums and social networking sites present a range of personal safety and privacy issues for young people, and there have been some serious cases highlighted in the media.

We use the resources, guidelines and materials offered by Kidsmart, as outlined above in the Safe use of the Internet section to teach children how to use chat rooms safely.

All commercial Instant Messaging and Social Networking sites are filtered as part of the LA Internet policy.

Pupils may take part in discussion forums or post messages on bulletin boards that teachers have evaluated as part of specific lesson activities. Individual pupil names or identifying information will never be used.

Internet-enabled mobile phones and handheld devices

More and more young people have access to sophisticated new internet-enabled devices such as SMART mobile phones, tablets and music players.

It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or weblog. Pupils will be taught the legal and moral implications of posting photos and personal information from mobile phones to public websites etc. and how the data protection and privacy laws apply.

- Pupils are not allowed to have personal mobile phones or other similar devices in school.
- Staff must NOT use personal mobile phones in lessons OR for taking photographs.
- Parents may request that such devices are kept at the School Office for pupils who may need them on their journey to and from school.
- Parents must NOT take photographs that include images of other children and upload these to social media sites.

Cyberbullying - Online bullying and harassment

Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on pupils. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy. These include:

- No access to public chat-rooms, Instant Messaging services and bulletin boards.
- Pupils are taught how to use the Internet safely and responsibly, and are given access to guidance and support resources from a variety of sources.

We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support pupils and their families.

- Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school child protection procedures.

Contact details and privacy

As specified elsewhere in this policy, pupil's personal details, identifying information, images or other sensitive details will never be used for any public Internet-based activity unless written permission has been obtained from a parent or legal guardian.
Pupils are taught that sharing this information with others can be dangerous – see Teaching the Safe Use of the Internet.

School and pupil websites – pictures and pupil input

As part of the ICT and wider curriculum, pupils may be involved in evaluating and designing web pages and web-based resources.

Any work that is published on a public website and attributed to members of our school community will reflect our school, and will therefore be carefully checked for mistakes, inaccuracies and inappropriate content.

Pupils may design and create personal web pages. These pages will generally only be made available to other school users, or as part of a password protected network or learning platform.

Where pupil websites are published on the wider Internet, perhaps as part of a project with another school, organisation etc., then identifying information will be removed, and images restricted.

Deliberate misuse of the Internet facilities

All pupils have discussed the rules for using the Internet safely and appropriately. These rules should displayed in each classroom and the ICT suite
Where a pupil is found to be using the Internet inappropriately, for example to download games or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse.

Sanctions will include:

Unsuitable material (e.g. online games, celebrity pictures, music downloads, sport websites etc.)

- Initial warning from class teacher
- Report to Headteacher
- Letter to parent/carer

Offensive material (e.g. pornographic images, racist, sexist or hate website or images etc.)

- Incident logged and reported to Head teacher
- Initial letter to parent/carer
- Removal of Internet privileges/username etc.
- Meeting with Parent/Carer to re-sign Internet use agreement
- Subsequent incidents will be treated very seriously by the Headteacher, and may result in exclusion and/or police involvement.

How will complaints regarding e-Safety be handled?

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

International scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- All incidents will be recorded
- Interview/counselling by class teacher, Senior Management Team, e-Safety Coordinator and Head Teacher.
- Informing parents or carers.
- Removal of Internet or computer access for a period of time.
- Referral to LA / Police.

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head Teacher.

Education - Parents/ Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- *Curriculum activities*
- *Letters, newsletters, web site,*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications E.g. www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers*

Education & Training – Staff / Volunteers

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

- **A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.**
- **All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.**
- *The E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.*
- *This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*
- *The E-Safety Coordinator will provide advice / guidance / training to individuals as required.*

Training – Governors

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

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

Technical and hardware guidance

School Internet provision
The school uses the standard LA Internet Service Provider, which is ICTS, as part of the Wolverhampton Council's Broadband consortium.
ICTS provides an always-on broadband connection at speeds up to 10 MB.

Content filter
The ICTS uses a sophisticated content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.

- All pupils and staff have been issued with clear guidelines on what to do if this happens and parents will be informed where necessary.
- Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.

Downloading files and applications
The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate and may adversely affect the performance and reliability of school equipment.

- Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member.

Portable storage media
Staff are allowed to use their own portable media storage (USB Keys etc.). If use of such a device results in an anti-virus message they should remove the device and immediately report to the ICT Co-ordinator.

Security and virus protection
The school subscribes to the Microsoft 'System Center Endpoint Protection'. The software is monitored and updated regularly by the school technical support staff.

- Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the ICT Co-ordinator.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

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

- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.**
- **All users will be provided with a username and secure password** by (*Alex Lane) who will keep an up to date record of users and their usernames.* **Users are responsible for the security of their username and password.**
- **The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place (e.g. school safe)**
- Alex Lane **is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations**
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- *The school has provided enhanced / differentiated user-level filtering*
- *School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.*
- *An appropriate system is in place for users to report any actual / potential technical incident / security breach to the Headteacher and E-Safety Coordinator, as agreed).*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- *An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.*
- *An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **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.

- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *pupils* in the digital / video images.
- *Staff are allowed to take digital / 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 taken on school equipment, the personal equipment of staff should not be used for such purposes.*
- *Care should be taken when taking digital / video images that students / 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*
- *Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.*
- *Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.*
- *Written permission from parents or carers will be obtained before photographs of pupils are published on the school website*
- *Pupil's work can only be published with the permission of the Pupil and parents or carers.*

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- **It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.**
- **Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.**
- **All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".**
- **It has a Data Protection Policy**
- **It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)**
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out

- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**
- **Transfer data using encryption and secure password protected devices.**

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

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

	Staff				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	lowed with staff permission	Not allowed
Mobile phones may be brought to school		X						X

Use of mobile phones in lessons				X				X
Use of mobile phones in social time		X						X
Taking photos on mobile phones / cameras				X				X
Use of other mobile devices e.g. tablets, gaming devices		X						X
Use of personal email addresses in school, or on school network				X				X
Use of school email for personal emails				X				X
Use of messaging apps				X				X
Use of social media				X				X
Use of blogs				X				X

When using communication technologies the school considers the following as good practice:

- **The official *school* email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** *Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).*
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- **Any digital communication between staff and students / pupils or parents / carers (email) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Whole class / group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.*
- *Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.

- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to Pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The *school's* use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	

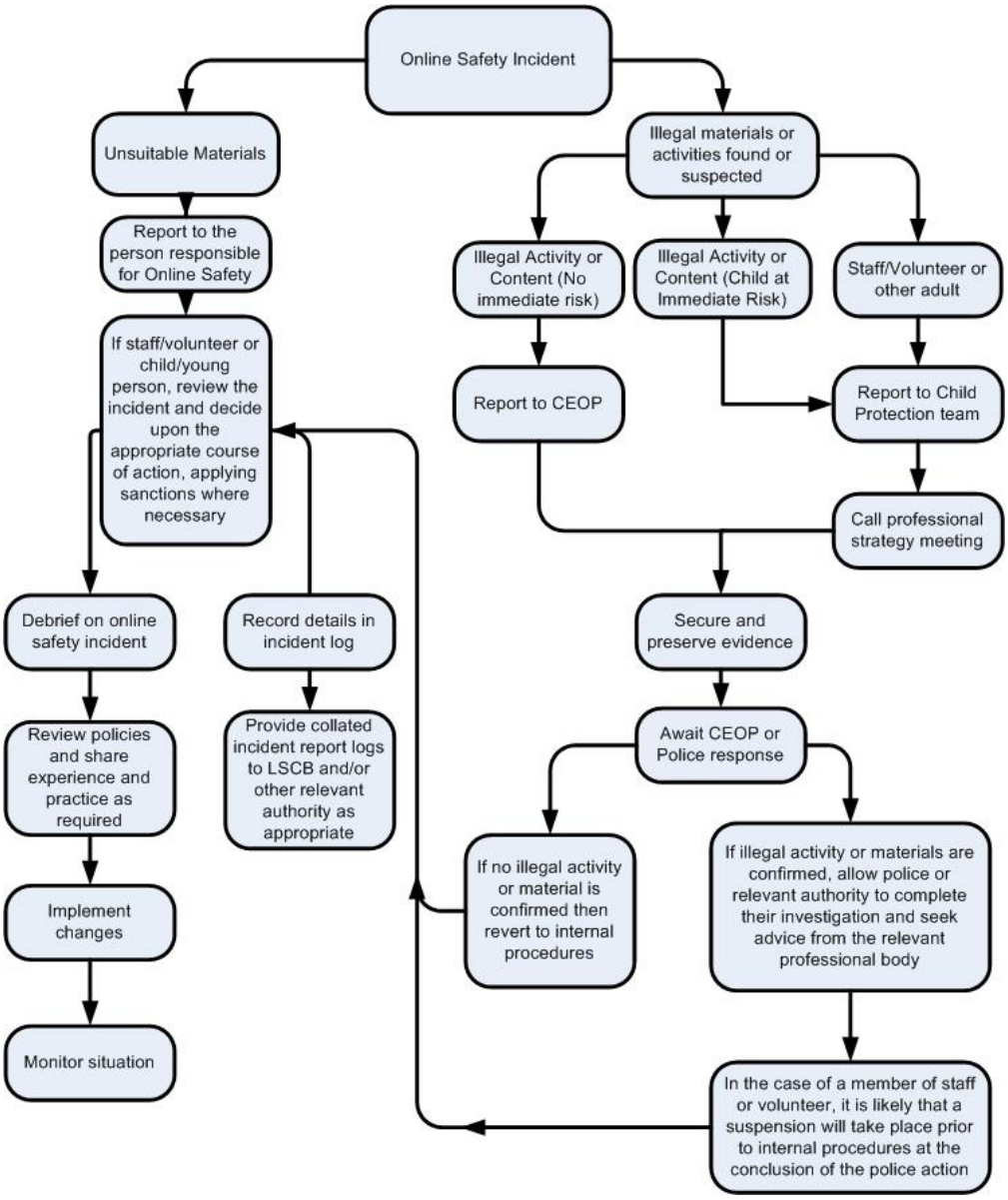
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non educational)		X			
On-line gambling				X	
On-line shopping / commerce				X	
File sharing		X			
Use of social media				X	
Use of messaging apps				X	
Use of video broadcasting e.g. YouTube			X		

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils — Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Phase Coordinator	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction s
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	X	X	X	X

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

Staff

Incidents:	Refer to Headteacher	Refer to Local Authority	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	X	X

Inappropriate personal use of the internet / social media / personal email	X			X	X		
Unauthorised downloading or uploading of files	X			X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X			X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X			X	X		
Deliberate actions to breach data protection or network security rules	X	X	X	X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X		X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X		X	X	X	X
Actions which could compromise the staff member's professional standing	X	X		X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X		X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X		X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X		X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X

Acknowledgements

The following range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this E-Safety Policy Template, are listed below:

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

Date Approved: _____

Signed: _____ Headteacher

Signed: _____ Chair of Governor

Appendices

Rakegate Primary School

Class Rules for responsible ICT use

Keep safe: Keep SMART

1. I will ask permission before using any ICT equipment (e.g. computers, ipads, digital cameras, etc.), and only use it when a teacher or another adult is with me.

2. I will only use the school's computers and ipads for schoolwork and homework.

3. I will not look at other people's files without their permission.

4. I will use the usernames and passwords provided by the school to access the school network.

5. I will not bring software or USB memory sticks into school without permission.

6. I will ask permission before using the Internet, and only use it when a staff member is present.

7. I will only visit web sites that I am asked to by school staff, or that have been saved in a shared internet link folder for pupils to use.

8. I will not use Google image search without being asked to do so by a school staff member.

9. I will not download anything (files, images etc.) from the Internet unless given permission.

10. I will only use an approved email account provided for me by the school to send email as part of my learning. I will not use personal email accounts (e.g. Hotmail, Yahoo) at school.

11. The messages I send or information I upload as part of my school work will always be polite.

12. I will not give my home address, phone number, send a photograph or video, or give any other personal information online that could be used to identify me, my family or my friends, unless my teacher has given permission.

13. If I see anything that makes me uncomfortable, or I receive a message I do not like, I will not respond to it but I will immediately tell a school staff member.

14. I will use the Kidsmart website to help me understand how to keep safe when using ICT.

15. I understand that the school may check my computer files, e-mail and the Internet sites I visit, to help keep me safe.

16. I understand that if I deliberately break these rules my parents and the Head Teacher will be informed.

Rakegate Primary School
iPad/Laptop Acceptable Use Policy for School

The policies, procedures and information within this document apply to all iPads, laptops or any other IT handheld device used in school. Teachers and other school staff may also set additional requirements for use within their classroom.

Users Responsibilities

- Teachers are required to set an enhanced password to prevent other users from misusing it.
- The ipad screen is made of glass and therefore is subject to cracking and breaking if misused: Never drop nor place heavy objects (books, laptops, etc.) on top of the ipad.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the ipad/laptop screen.
- Do not subject the ipad/laptop to extreme heat or cold.
- Do not store or leave unattended in vehicles.
- Users may not photograph any other person, without that persons' consent.
- Consent must be acquired from parents/carers before displaying or publishing children's photographs (i.e. through parental consent forms given at the start of each academic year)
- The ipad/laptop is subject to routine monitoring by Rakegate Primary School. Devices must be surrendered immediately upon request by any member of staff.
- Users in breach of the E-Safety policy may be subject to but not limited to; disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.

Safeguarding and Maintaining as an Academic Tool

- ipad batteries are required to be charged and be ready to use in school.
- Syncing the ipad to iTunes and other Mobile Device Management software will be controlled by the IT Staff.
- Items deleted from the ipad may not be recovered.
- The whereabouts of the ipad should be known at all times.
- It is a user's responsibility to keep their ipad/laptop safe and secure.
- Ipads/laptops belonging to other users are not to be tampered within any manner.
- If an ipad/laptop is found unattended, it should be given to the nearest member of staff.

Lost, Damaged or Stolen ipad/laptop

- If the ipad/laptop is lost, stolen, or damaged, the ICT Technician/Computing Coordinator/Head Teacher must be notified immediately.
- Ipads/laptops that are believed to be stolen can be tracked through various systems at the school.

Prohibited Uses

- Accessing Inappropriate Materials – All material on the iPad/laptop must adhere to the ICT Responsible Use Policy. Users are not allowed to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.
- Illegal Activities – Use of the school's internet/e-mail accounts for financial or commercial gain or for any illegal activity.
- Violating Copyrights – Users are not allowed to have music and install apps on their iPad unless they have sought permission first.
- Cameras – Users must use good judgment when using the camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way.
- Images of other people may only be made with the permission of those in the photograph.
- Posting of images/movie on the Internet into a public forum is strictly forbidden, without the express permission of the Teacher or in the case of staff use; a member of the Senior Leadership team.

- Misuse of Passwords, Codes or other Unauthorised Access: Any user caught trying to gain access to another user's accounts, files or data will be subject to disciplinary action.
- Inappropriate media may not be used as a screensaver or background photo. Presence of pornographic materials, inappropriate language, alcohol or drug related symbols or pictures will result in disciplinary actions.
- Individual users are responsible for the setting up and use of any home internet connections and no support will be provided for this by the school.
- Users should be aware of and abide by the guidelines set out by the School E-Safety policy.
- Rakegate Primary School reserves the right to confiscate and search an ipad/laptop to ensure compliance with this E-safety Policy.

Home Use

Users are not allowed to grant anyone access to your iPad.
Only work related usage is permitted.
The camera and other features should not be used for personal use.

I agree to adhere to the Rakegate's ipad/Laptop Usage Policy:-

Name:

Signed:

Date:

ipad Serial Number:

Laptop Serial Number:

Rakegate Primary School

Acceptable User Policy - Infants

I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not load photographs of myself onto the computer
- never agree to meet a stranger

Anything I do on the computer may be seen by someone else

Names:

Date: _____

Rakegate Primary School
Acceptable User Policy - Juniors

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only visit sites which are appropriate to my work at the time
- work in collaboration only with friends and I will deny access to others
- tell a responsible adult straight away if anything makes me feel scared or uncomfortable online
- make sure all messages I send are respectful
- show a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend
- only email people I know or those approved by a responsible adult
- only use email which has been provided by school
- talk to a responsible adult before joining chat rooms or networking sites
- always keep my personal details private. (My name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult and my parents before I show photographs of myself
- never meet an online friend without taking a responsible adult that I know with me
- I know that once I post a message or an item on the internet then it is completely out of my control.
- I know that anything I write or say or any website that I visit may be being viewed by a responsible adult

Names:

Date: _____

Staff Laptop and ICT Equipment Loan Agreement

I have borrowed a school laptop to use out of school in agreement with both Head Teacher and the Computing coordinator or Computing Technician.

Make: _____

Model: _____

Serial number: _____

It is understood that I will return the equipment to school if requested to do so by either the Head Teacher, Computing coordinator or Computing Technician

I undertake to take proper care of the equipment whilst in my possession and will abide by the requirements of the school's insurance policy with regard to protecting the equipment from loss or damage. I agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, I will replace or arrange for the repair of the equipment at my own expense.
I will use the equipment in accordance with the schools e-Safety Policy and Staff Acceptable Use policy.

I agree to the above conditions:

(Signature) _____

(Print name) _____ Date:_____

Returned: _____ Date:_____