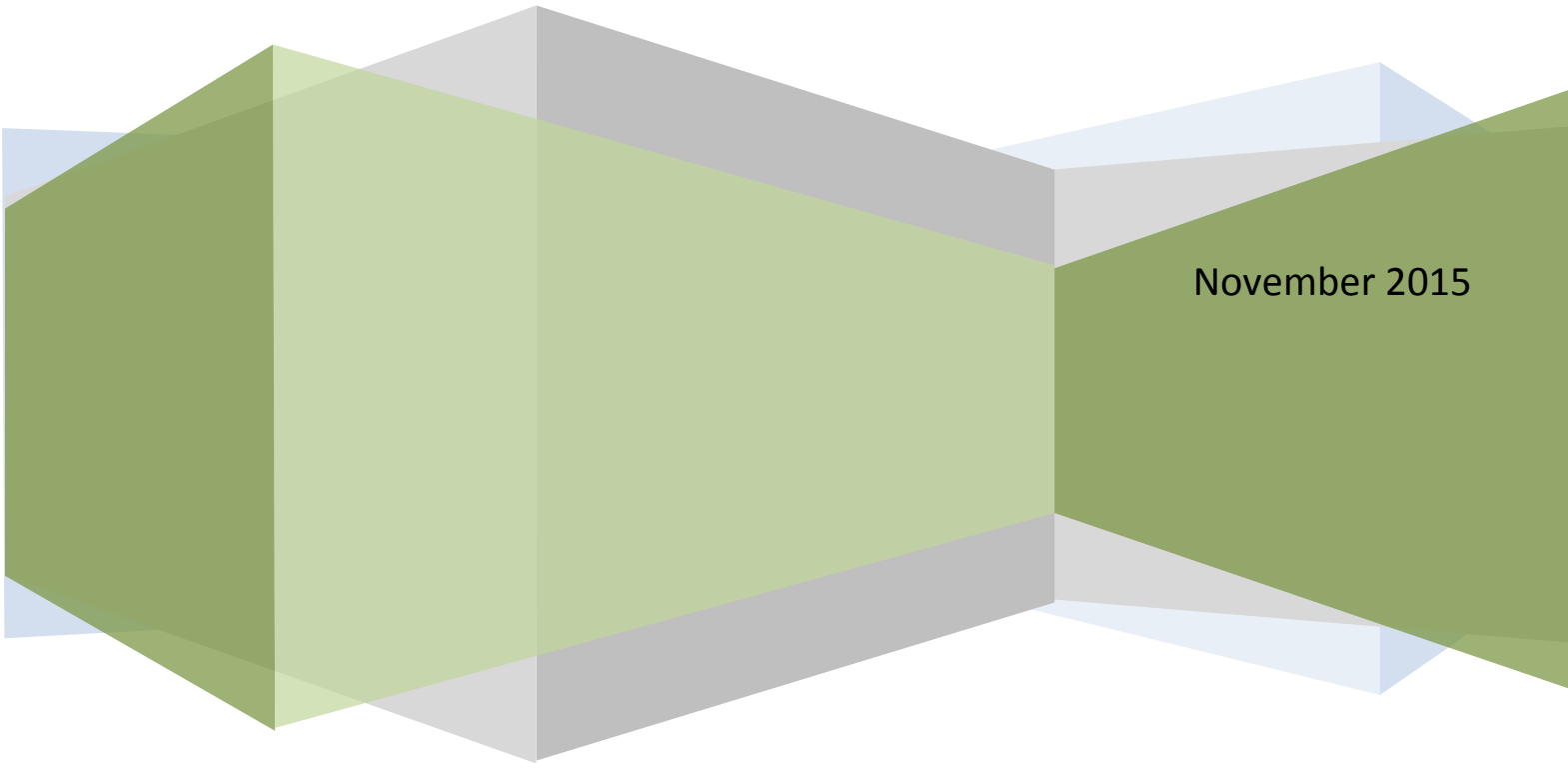
Gig Mill Primary School

E-Safety Policy and Guidelines



November 2015

Gig Mill Primary School

E-Safety Advice and Guidance

Rationale

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school E-Safety policy should help to ensure safe and appropriate use. The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks.

Scope

This guidance applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. This policy should be reviewed in line with the School Information Security Policy.

Development, Monitoring and Review of the E-Safety Policy:

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

- School E-Safety Coordinator
- Head teacher / Senior Leaders
- Teachers
- ICT Technical staff
- Governors

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

- Staff meetings
- School / Student / Pupil Council
- INSET Days
- Governors meetings / sub-committee meetings
- School website / newsletters

The school will monitor the impact of the policy using**:**

- Logs of reported incidents
- DGfL or internal monitoring logs of internet activity (including sites visited)
- Surveys / questionnaires of stakeholders

Roles and Responsibilities

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 E-Safety Governor.

The role of the E-Safety Governor will include:

- Regular meetings with the E-Safety Co-ordinator / committee
- Regular updates on the monitoring of E-Safety incident logs
- Reporting to relevant Governor committees / meetings

Head teacher and Senior Leaders:

The Head teacher is responsible for ensuring the safety (including E-Safety) of members of the school community and is likely to be the school's Senior Information Risk Owner (SIRO) The schools SIRO is responsible for reporting security incidents as outlined in the schools Information Security Policy. The day to day responsibility for E-Safety will be delegated to the E-Safety Co-ordinator / ICT technician.

- The Head teacher /SLT are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff, receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant. They are also responsible for ensuring that pupils and students are taught how to use ICT tools such as the internet, email and social networking sites, safely and appropriately
- The Head teacher / SLT 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 SLT will receive regular monitoring reports from the E-Safety Co-ordinator / Officer
- The Head teacher and another member of the SLT 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
- The Head teacher is responsible for ensuring that parents and carers, when given access to data and information relating to their child/children via the learning platform, have adequate information and guidance relating to the safe and appropriate use of this on line facility

E-Safety Coordinator / Officer:

The school has a named person with the day to day responsibilities for E-Safety. Responsibilities include:

- Leading the E-Safety committee
- Taking day to day responsibility for E-Safety issues and having a leading role in 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 taking place.
- Providing training and advice for staff
- Liaising with the Local Authority
- Liaising with the schools SIRO to ensure all school data and information is kept safe and secure
- Liaising with school ICT technical staff and/or school contact from the managed service provider- RM
- Receiving reports of E-Safety incidents and creating a log of incidents to inform future E-Safety developments
- Meeting regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering
- Reporting regularly to Senior Leadership Team

Managed service provider:

The managed service provider is responsible for helping the school to ensure that it meets the E-Safety technical requirements outlined by DGfL. The managed service provides a number of tools to schools including, Smartcache servers, Securus (optional), SafetyNet Universal, which are designed to help schools keep users safe when on-line in school. Schools are able to configure many of these locally or can choose to keep standard settings.

The DGfL Client team work with school representatives to develop and update a range of Acceptable Use Policies and any relevant Local Authority E-Safety policy and guidance. These can be accessed either on DVRC or via the E-Safety interest space on the portal.

Members of the DGfL team will support schools to improve their E-Safety strategy
The managed service provider maintains backups of email traffic for 90 days. If access to this information is required, the school should contact the DGfL team.

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 encourage pupils to develop good habits when using ICT to keep themselves safe
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP)

- They report any suspected misuse or problem to the E-Safety Co-ordinator / Head teacher / Senior Leader / Head of ICT / ICT Co-ordinator / Class teacher / for investigation / action / sanction
- Digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) 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 school activities
- Students / pupils understand and follow the school E-Safety and acceptable use policy
- Students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned, students / 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. They include the teaching of E-Safety in their lessons

Designated person for Child Protection / Child Protection Officer:

The named person is trained in E-Safety issues and is aware of the potential for serious child protection 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 Committee:

Members of the E-Safety committee will assist the E-Safety Coordinator with:

- The production / review / monitoring of the school E-Safety policy / documents
- The production / review / monitoring of the managed service/school filtering policy
- Will endeavour to meet at least twice annually

Students / pupils:

Students/pupils have access to the school network and technologies that enable them to communicate with others beyond the school environment. The network is a secure and safe system provided through DGfL. Students/pupils:

- Are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy which they will be expected to sign on paper (and then on screen every 60 days) before being given access to school systems
- Need to 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images, use of social networking sites 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 the use of an externally available web based system, provided by 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 therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national / local E-Safety campaigns / literature

Parents and carers will be responsible for:

- Endorsing (by signature) the Student / Pupil Acceptable Use Policy
- Accessing the school website / Learning Platform/ on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

Community Users/ 'Guest Access':

Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems-see appendix 3.

Policy Statement

Education – students / pupils

There is a planned and progressive E-Safety/E-literacy curriculum. Learning opportunities are embedded into the curriculum throughout the school and are taught in all year groups. E-Safety education is provided in the following ways:

- A planned E-Safety/E-literacy programme is provided as part of ICT / PHSE and is regularly revisited – this include the use of ICT and new technologies in school and outside school
- Key E-Safety messages are reinforced as part of assemblies
- Students / pupils are 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
- Students / pupils are aware of the Student / Pupil AUP and are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students / pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet are posted in all rooms
- Students and pupils are taught the importance of information security and the need to keep information such as their password safe and secure
- Staff act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

The school provides information and awareness to parents and carers through:

- Letters, newsletters, web site, Learning Platform
- Parents evenings / presentations
- Reference to the DGfL E-Safety interest space in the Learning Platform

Education - Extended Schools

The school offers family learning meetings in ICT, digital literacy and E-Safety so that parents and children can together gain a better understanding of these issues. Messages to the public around E- Safety are targeted towards grandparents and other relatives as well as parents.
Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff

All staff receive regular E-Safety training and understand their responsibilities, as outlined in this policy. Training is offered as follows:

- A planned programme of formal E-Safety training is made available to staff. An audit of the E-Safety training needs of all staff is carried out regularly. It is expected that some staff will identify E-Safety as a training need within the performance management process

- All new staff receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Policies
- The E-Safety Coordinator (or other nominated person) receives regular updates through attendance at DGfL / LA training sessions and by reviewing guidance documents released by DfE / DGfL / LA and others.
- This E-Safety policy and its updates are presented to and discussed by staff in staff meetings / INSET days
- The E-Safety Coordinator provides advice / guidance / training as required to individuals

All staff are familiar with the schools' Policy including:

- Safe use of e-mail
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network
- Safe use of school network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- Publication of pupil information/photographs and use of website
- Cyberbullying procedures
- Their role in providing E-Safety education for pupils
- The need to keep personal information secure

Staff are reminded / updated about E-Safety matters at least once a year.

Training – Governors

Governors take part in E-Safety training / awareness sessions

.

This is offered by:

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

Technical – infrastructure / equipment, filtering and monitoring

The managed service provider is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible. The school is responsible for ensuring that policies and procedures approved within this policy are implemented.

School ICT systems will be managed in ways that ensure that the school meets the E-Safety technical requirements outlined in the Acceptable Use Policies

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted

All users will have clearly defined access rights to school ICT systems

- All users will be provided with a username and password
- Users will be made responsible for the security of their username and password. They must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security

- The school maintains and supports the managed filtering service provided by DGfL
- The school can provide enhanced user-level filtering through the use of the SmartCache/SafetyNet Universal
- The school manages and updates filtering issues through the RM helpdesk
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager/appropriate member of staff. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual / potential E-Safety incident to the relevant person
- The managed service provider ensures that appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- An agreed procedure is in place for the provision of temporary access to "guests" (eg trainee teachers, visitors) onto the school system
- An agreed procedure is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices
- The school infrastructure and individual workstations are protected by up to date virus software
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

Curriculum

E-Safety is a focus in all areas of the curriculum and staff re-enforce E-Safety messages in the use of ICT across the curriculum.

- In lessons, where internet use is pre-planned, students / pupils are guided to sites checked as suitable for their use and there are processes in place for dealing with any unsuitable material that is found in internet searches
- Where students / pupils are allowed to freely search the internet, eg using search engines, staff should monitor the content of the websites the young people visit
- The school provides opportunities within a range of curriculum areas to teach about E-Safety
- Students / pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- Students / pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Child line or CEOP report abuse button

Use of digital and video images

When using digital images, staff inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They recognise the risks attached to publishing their own images on the internet eg on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, and follow school policies concerning the sharing, distribution and publication of those images. Those images are only taken on school equipment, the personal equipment of staff are not used for such purposes
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However with the express permission of the Head teacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupil's device.
- Care is taken when capturing digital / video images, ensuring students / pupils are appropriately dressed and that they are not participating in activities that might bring the individuals or the school into disrepute
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and comply with good practice guidance on the use of such images
- Students' / pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers is obtained before photographs of students / pupils are published on the school website
- Student's / pupil's work can only be published with the permission of the student / pupil and parents or carers. Parents should have signed the DSCB consent form

Data Protection

Personal data will is 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.

Staff are aware of the Dudley Information Security Policy. A breach of the Data Protection Act may result in the school or an individual fine of up to £500000

Staff ensure that they:

- Take care at all times, to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Access personal data on secure password protected computers and other devices or via the Learning Platform 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, USB 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 once it has been transferred or its use is complete.

Communications

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. Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems eg by remote access from home
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE 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 programmes must not be used for these communications
- Students / pupils are provided with individual school email addresses for educational use
- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff
- Mobile phones may not be brought into school by pupils/students
- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances should a member of staff contact a pupil or parent/ carer using their personal device unless authorised to do so by the school.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device
- The school provides a safe and secure way of using chat rooms, blogs and other 'social networking technologies' via the Learning Platform. Other 'social networking' facilities may be 'unfiltered' for curriculum purposes. Staff are aware of the procedure they need to follow when requesting access to externally based social networking sites

Unsuitable / inappropriate activities

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

The school will take all reasonable precautions to ensure E-Safety.
However, owing to the 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.

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

- Interview/counselling E-Safety Coordinator / Head teacher.
- Informing parents or carers.
- Removal of Internet or computer access for a period.
- Referral to LA / Police.

The LA has set out the reporting procedure for E-Safety incidents (see Appendix 1).

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

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Date the Policy was approved by Governors …….

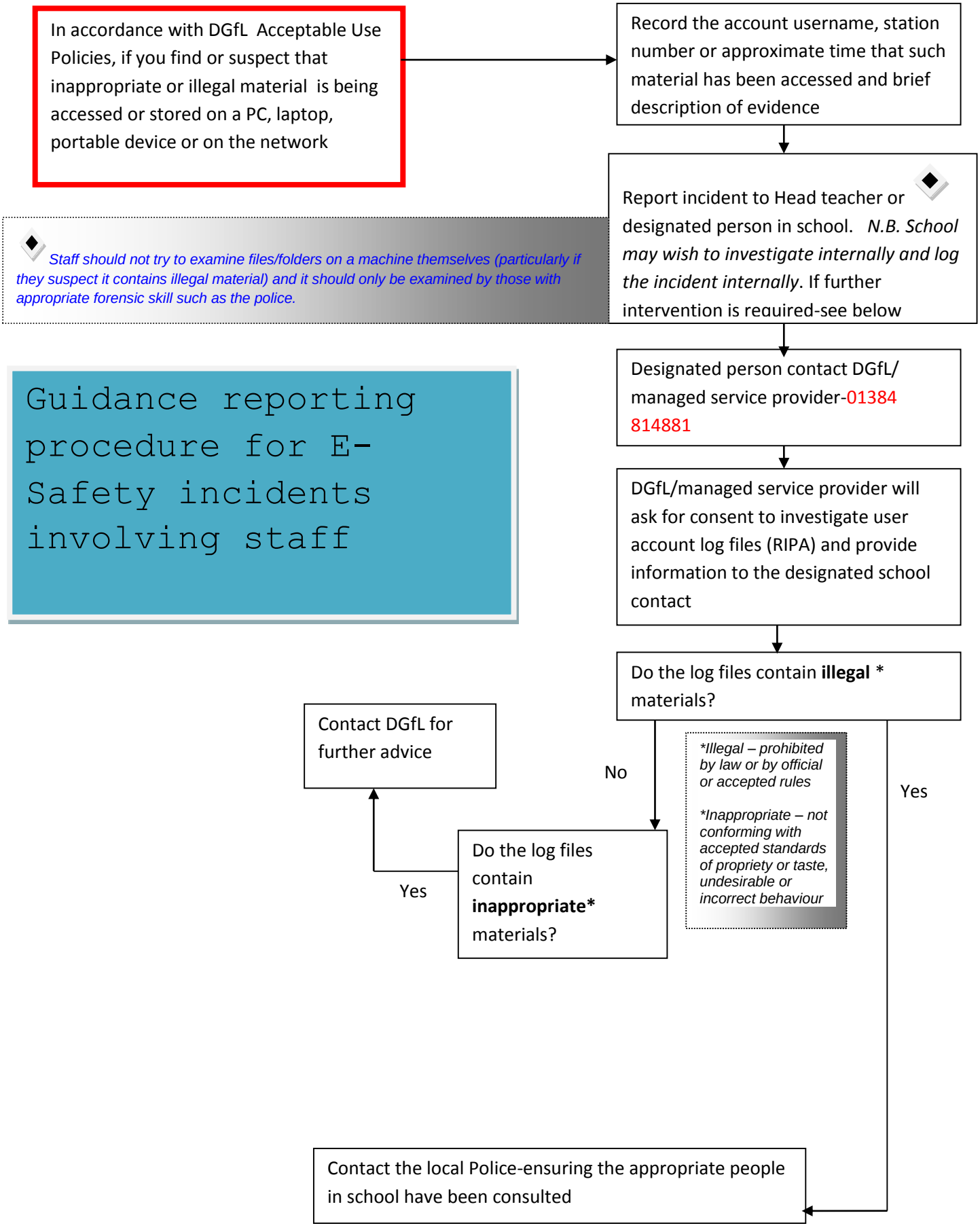
Date for review ……..

Contact ……..

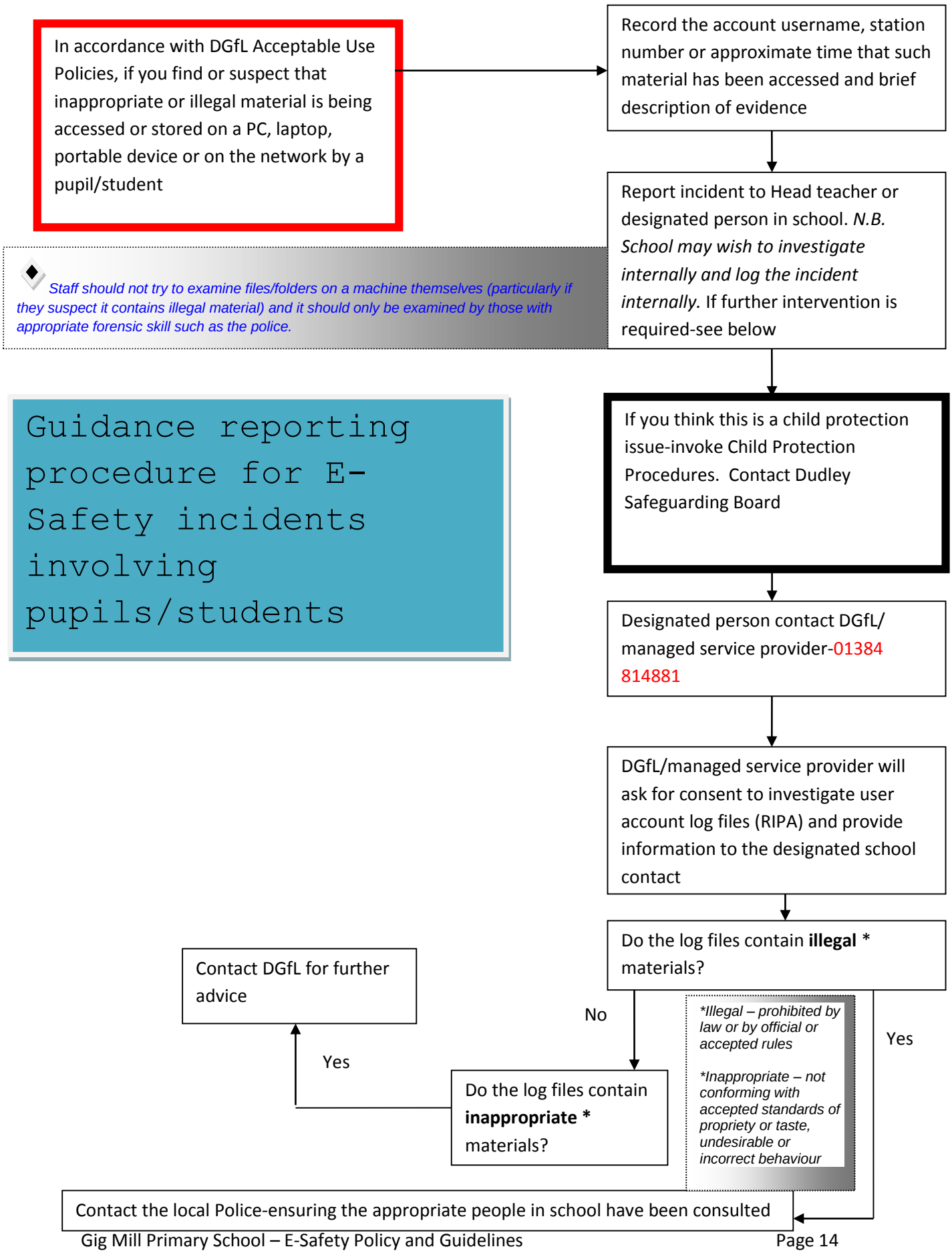
This E-Safety Guidance and Policy has been written with references to the following sources of information:

BECTA
Dudley LA
Hertfordshire E-Safety Policy
Kent e-Safety Policies, Information and Guidance
South West Grid For Learning- School E-Safety Policy

Appendix 1- Guidance procedure for E-Safety incidents-Staff user incidents



Appendix 1 -Guidance procedure for E-Safety incidents-Pupil user incidents



Appendix 2-E-Safety tools available on the DGfL network

E-Safety tool	**Type**	**Availability**	**Where**	**Details**
Smartcache/ SafetyNet Universal	Web filtering	Provided as part of DGfL	All network connected devices within DGfL	Gives schools the ability to audit, filter and un-filter websites
RM Tutor	Teacher support	Provided as part of DGfL	Managed school desktops	Allows teachers to view and demonstrate screens, control hardware and distribute work
CC4 AUP	Awareness raising	Part of CC4-needs to be enabled	All CC4 stations at log in	When enabled through the management console, users are given an acceptable use policy at log in
Securus (optional implementation)	Monitoring software-*licenses available on Linux and Apple devices(early 2011)*	Available to all schools who sign an agreement and attend training	All school XP desktops and networked laptops	Takes a snapshot of a screen when an event is triggered. A range of events can be monitored
Email	Filtering and list control	Provided as part of DGfL	Easymail/ Live@edu	Allows schools to restrict where email is sent from/to
RM Password Plus	Safe practice	Provided as part of DGfL3	All CC4 stations	A password management tool that enforces password rules of complexity and length for different users

Appendix 3

Gig Mill Primary School

Rules for Responsible Internet Use

For Primary Pupils

The school has installed computers and provided Internet access to help our learning. I understand that the school may check my computer files and may monitor any Internet sites I visit.

These rules will keep everyone safe and help us to be fair to others. It is important that you read this policy carefully. If there is anything that you do not understand, please ask.

I agree that:

I will not share any of my passwords with anyone, or use another person's password. If I find out someone else's password, I will tell that person and a member of the school staff so they can change it.

I will use a password which contains some small and some big (capital) letters plus a number or a symbol *e.g Skool5 or com**2er* and change it on a regular basis.

I will use the technology at school for learning. I will use the equipment properly and not interfere, change or delete someone else's work.

If I use a flash drive or other storage device, I will follow school guidelines on their use.

I will only e-mail people I know, or my teacher has approved.

If I attach a file to an email, it will not include any inappropriate materials (something I would not want my teacher to see or read) or anything that threatens the integrity of the school ICT system.

I will be respectful in how I talk to and work with others online and never write or participate in online bullying. If anyone sends me a message I do not like or feel uncomfortable about I will show it to my teacher or parent.

I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself.

I will not download any programmes or games on to the school computers, netbooks or laptops unless I have permission to do so.

I will always check with a responsible adult before I share or publish images of myself, my friends or other people onto the internet.

I will not make audio or video recordings of another pupil or teacher without their permission.

When using sites on the internet, I will not give my name, home address, telephone/mobile number, pretend to be someone else or arrange to meet someone I do not know, unless my parent, carer or teacher has given permission.

I will always follow the 'terms and conditions' when using a site. The content on the web is someone's property and I will ask my teacher to help me get permission if I want to use information, pictures, video, music or sound files.

I will think carefully about what I read on the Internet, question if it is from a reliable source and use the information to help me answer any questions (I should not copy and paste the information and say it's my own work).

If I want to connect my own device to the school network I will check with my teacher to see if it is possible.

I am aware of the CEOP report button and know when to use it.

I know anything I do on the computer may be seen by someone else.

Signed:……

PRINT NAME……

Dated: ……..

Appendix 3

Gig Mill Primary School

Staff Acceptable Use policy

Rules for Responsible Internet use

This policy applies to all adult users of the schools systems. We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this Policy.

It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Head Teacher or your line manager. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the Head Teacher

Any inappropriate use of the School's internet & e-mail systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal. Electronic information can be produced in court in the same way as oral or written statements.

Research Machines (RM) has a contractual obligation to monitor the use of the internet and e-mail services provided as part of DGfL, in line with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. RM, Dudley MBC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from employees the facility to view, send and receive electronic communications or to access the internet.

All information relating to our pupils, parents and staff is personal. You must treat all school information with the utmost care whether held on paper or electronically.

Official school systems must be used at all times.

Use of the Internet and Intranet

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- unauthorised access to computer material i.e. hacking;
- unauthorised modification of computer material; and
- unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply:-

- If you download any image, text or material check if it is copyright protected. If it is then follow the school procedure for using copyright material.
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to a senior member of staff.

- If you want to download any software, first seek permission from the Head Teacher and/or member of staff responsible /RM. They should check that the source is safe and appropriately licensed.
- If you are involved in creating, amending or deleting web pages or content on the web site, such actions should be consistent with your responsibilities and be in the best interests of the School.
- You should not :
    - introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
    - seek to gain access to restricted areas of the network;
    - knowingly seek to access data which you are not authorised to view;
    - introduce any form of computer viruses;
    - carry out other hacking activities.

Electronic Mail

Care must be taken when using e-mail as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school.
Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your head teacher. Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the School's business purposes which include the following:

1. providing evidence of business transactions;
2. making sure the School's business procedures are adhered to;
3. training and monitoring standards of service;
4. preventing or detecting unauthorised use of the communications systems or criminal activities;
5. maintaining the effective operation of communication systems.

In line with this policy the following statements apply:-

- You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.
- Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is 'Confidential' in the subject line.
- Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.
- Do not impersonate any other person when using e-mail or amend any messages received.
- Sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.
- It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.
- If the email is personal, it is good practice to use the word 'personal' in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.

- Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your headteacher.
- All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

Social networking

The use of social networking sites for business and personal use is increasing. Access to social networking sites is blocked on the school systems, however a school can manage access by un-filtering specific sites, internet usage is still monitored.

School staff may need to request access to social networking sites for a number of reasons including:

- Advertising the school or managing an 'official' school presence,
- For monitoring and viewing activities on other sites
- For communication with specific groups of adult users e'g a parent group.

Social networking applications include but are not limited to:

- Blogs
- Any online discussion forums, including professional forums
- Collaborative spaces such as Wikipedia
- Media sharing services e.g YouTube, Flickr
- 'Microblogging' applications e.g Twitter

When using school approved social networking sites the following statements apply:-

- School equipment should not be used for any personal social networking use
- Staff must not accept friendships from underage pupils. The legal age for students to register with a social networking site is usually 13 years; be aware that some users may be 13 or younger but have indicated they are older.
- It is important to ensure that members of the public and other users know when a social networking application is being used for official school business. Staff must use only their @<schoolname>. dudley.sch.uk email address or other school approved email mechanism and ensure all contributions are professional and uphold the reputation of the school
- Social networking applications should not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Postings should not be critical or abusive towards the school, staff, pupils or parents or used to place a pupil, student or vulnerable adult at risk of harm
- The social networking site should not be used for the promotion of personal financial interests, commercial ventures or personal campaigns, or in an abusive or hateful way
- Ensure that the appropriate privacy levels are set. Consider the privacy and safety settings available across all aspects of the service – including photos, blog entries and image galleries. Failing to set appropriate privacy levels could result in messages which are defamatory, libellous or obscene appearing on your profile before you have chance to remove them
- It should not breach the schools Information Security policy

Data protection

The processing of personal data is governed by the Data Protection Act 1998. Schools are defined in law as separate legal entities for the purposes of complying with the Data Protection Act. Therefore, it is the responsibility of the School, and not the Local Authority, to ensure that compliance is achieved.
As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the School. The main advantage of the internet and e-mail is that they provide routes to access and disseminate information.

Through your work personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the School*'s* premises or working remotely you must:-

- keep the data private and confidential and you must not disclose information to any other person unless authorised to do so. If in doubt ask your Head Teacher or line manager;
- familiarise yourself with the provisions of the Data Protection Act 1998 and comply with its provisions;
- familiarise yourself with all appropriate school policies and procedures;
- not make personal or other inappropriate remarks about staff, pupils, parents or colleagues on manual files or computer records. The individuals have the right to see all information the School holds on them subject to any exemptions that may apply.

If you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable.

I have read through and fully understand the terms of the policy. I also understand that the school may amend this policy from time to time and that I will be issued with an amended copy.

Signed:……

PRINT NAME……

Dated: ……..

Gig Mill Primary School

Community User- Acceptable Use policy

Rules for Responsible Internet use

This policy applies to all community users of the schools systems, who have guest access to the internet. We trust you to use the ICT facilities sensibly, professionally, lawfully, and in accordance with this Policy.
It is important that you read this policy carefully. If there is anything that you do not understand, please ask. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the school office.
Research Machines (RM) has a contractual obligation to monitor the use of the internet and e-mail services provided as part of DGfL, in line with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and RM, Dudley MBC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request.

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying our school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- unauthorised access to computer material i.e. hacking;
- unauthorised modification of computer material; and
- unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply:-

- Do not download any image, text or material which is copyright protected without the appropriate authorisation.
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to a member of staff
- If you want to download any software, first seek permission from the member of staff responsible. They should check that the source is safe and appropriately licensed.
- You should not :
    - introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
    - seek to gain access to restricted areas of the network;
    - knowingly seek to access data which you are not authorised to view;
    - introduce any form of computer viruses;

I have read through and fully understand the terms of the policy. I also understand that the school may amend this policy from time to time and that I will be issued with an amended copy.

Signed:……

PRINT NAME……

Dated: ……..