Peters Hill Primary

Ambition Belief Compassion Pride Respect

Online Safety Policy and Guidance

October 2017

Responsibility	Head Teacher
To be reviewed	Annually
Other Policies Related	Child Protection Safeguarding Educational Visits Health & Safety Anti Bullying

Table of Contents

Scope of Policy

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 will be reviewed in line with the School Information Security Policy.

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)
- Internal monitoring of data for network activity
- Surveys/questionnaires

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the full Governing Body or Governors' Sub Committees (if/where appropriate) receiving regular information about Online Safety incidents and monitoring reports. The Governing Body will review its Online Safety Policy at the start of each academic year to ensure that all new staff and pupils are aware of its content and have signed appropriate Acceptable Use Policies.

A member of the Governing Body, as safeguarding lead has the role of Online Safety Governor.

The role of the Online Safety Governor will include:

Regular meetings with the Online Safety Co-ordinator/school safeguarding lead Regular updates on the monitoring of Online Safety incident logs

Regular updates on the monitoring of the filtering of web sites Reporting to relevant Governor meetings

Head teacher and Senior Leaders:

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

The Head teacher/SLT are responsible for ensuring that the Online Safety Coordinator /ICT Co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their Online 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 Online 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 monitoring reports from the Online Safety/ICT Co-ordinator on an as and when basis.

The Headteacher and Deputy Headteacher as safeguarding leads should be aware of the procedures to be followed in the event of a serious Online 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 any learning platform, have adequate information and guidance relating to the safe and appropriate use of this on line facility.

Online Safety/ICT Coordinator: Lynsey Graham/Tracy Curnin

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

- Leading the Online Safety working group
- Taking day to day responsibility for Online Safety issues and having a leading role in establishing and reviewing the school Online Safety policies/documents
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- Providing training and advice for staff Liaising with the Local Authority
- Liaising with the school's SIRO to ensure all school data and information is kept safe and secure
- Liaising with school office and/or school contact from the managed service provider- RM
- Receiving reports of Online Safety incidents and creating a log of incidents to inform future Online Safety developments
- Meeting regularly with the Online Safety/Safeguarding Governor to discuss current issues, review incident logs and filtering
- Attending relevant meetings/Governor meetings as required 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 Online Safety technical requirements outlined by DGfL. The managed service provides a number of tools to school's including, Smoothwall and E-Safe which are designed to help school's 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 Online Safety policy and guidance. These can be accessed either on DVRC or via the Online Safety interest space at http://safeguarding.dudley.gov.uk/search/?q=E+Safety

Members of the DGfL team will support school's 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 Online Safety matters and of the current school Online 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 Online Safety/ICT Co-ordinator/Headteacher/Senior Leader/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.
- Online Safety issues are embedded in all aspects of the curriculum and other school activities.
- Students/pupils understand and follow the school Online 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 Online 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 school safeguarding lead (person for Child Protection/Child Protection Officer):

The named person is trained in Online 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

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 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 and information about national/local E Safety campaigns/literature etc.

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 in future 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. (*Guest access to the internet in school will be subject to the same filtering rules as other school users. No access provided to school software. There will be no access to pupil or staff data or information unless relevant parties have agreed. The school retains the right to check portable storage devices such as memory sticks before they are attached to the school network).*

Policy Statement

Education – students/pupils

There is a planned and progressive E Safety curriculum. Learning opportunities are embedded into the curriculum throughout the school and are taught in all year groups.

- Online Safety education is provided in the following ways:
- A planned Online Safety programme is provided as part of ICT/PHSE/other lessons and is regularly revisited – this includes the use of ICT and new technologies in school and outside school
- Key Online Safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- 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 Outside agencies.

Education – parents/carers

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

- Letters, newsletters, web site
- Social Media (Twitter), Blogging (Wordpress)
- Parents'/Carers' Evenings/workshops

Education - Extended Schools

The school offers family learning workshops in ICT, digital literacy and Online 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 E Safety training and understand their responsibilities, as outlined in this policy. Training is offered as follows:

- A programme of formal Online Safety training is made available to staff. Needs are identified by an audit carried out by the ICT Coordinator on a regular basis It is expected that some staff will identify E Safety as a training need within the appraisal process
- New staff receive Online Safety guidance as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Policies and training is available
- The Online Safety/ICT Coordinator receives regular updates through attendance at DGfL/LA/other information/training sessions and by reviewing guidance documents released by DfE/DGfL/LA and others.
- This Online Safety Policy and its updates are presented to and discussed by staff in staff/team meetings etc
- The Online Safety/ICT Coordinator provides advice/guidance/training as required to individuals

All staff are familiar with the school's 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 procedure.
- 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 are invited to take part in Online Safety training/awareness sessions, particularly those who are members of any sub-committee/group who are involved in ICT/ Online Safety/health and safety/child protection/safeguarding matters

This is offered by:

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

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 Online 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 required to change their password every 90 days as advised by school via e-mail instruction. *(In early years we choose to use group or class log-ons and passwords for FS (Foundation Stage) pupils, but staff are aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy and the AUP)*
- 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 (Smoothwall)
- 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 (S. Parsons). If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by (the Online Safety working group).
- Remote management tools are available to staff to control workstations and view users activity.
- An appropriate system is in place for users to report any actual/potential Online 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 (to be described) regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on laptops and other portable devices that may be used out of school
- An agreed procedure is in place (reference in AUP) 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

Online Safety is a focus in all areas of the curriculum and staff re-enforce Online 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- *(The school may use ICE, a search engine, to ensure pupil's access to the web is safe).*

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 Online Safety. It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager or managed service provider temporarily remove those sites from the filtered list for the period of study. Any requests to do so are auditable and should be logged.

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 Childline 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.

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 (in line with Dudley Safeguarding Children's Board-DSCB consent form).

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:

- Fairlyand lawfully 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 £500,000

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 (delete as appropriate), 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 *(as many memory sticks/cards and other mobile devices cannot 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. *(Data storage on removal media is not allowed, even if encrypted – some organisations do not allow storage of personal data on removable devices).*

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- *(If staff use none standard or personal email accounts these are not secure and cannot always be monitored)*

- 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 communication.
- Students/pupils are provided with individual school email addresses for educational use (delete/amend as appropriate

- 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; any who do have their phones placed in school safe until collection at end of school day

- Pupils are NOT allowed to bring personal mobile devices/phones to school

- 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 Online 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 by mentor/ class teacher/E Safety/ICT Coordinator/Head teacher/safeguarding lead.
- Informing parents or carers.
- Removal of Internet or computer access for a period, (which could ultimately prevent access to files held on the system, including examination coursework).

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.

Approved by Full Governing Body – October 2015

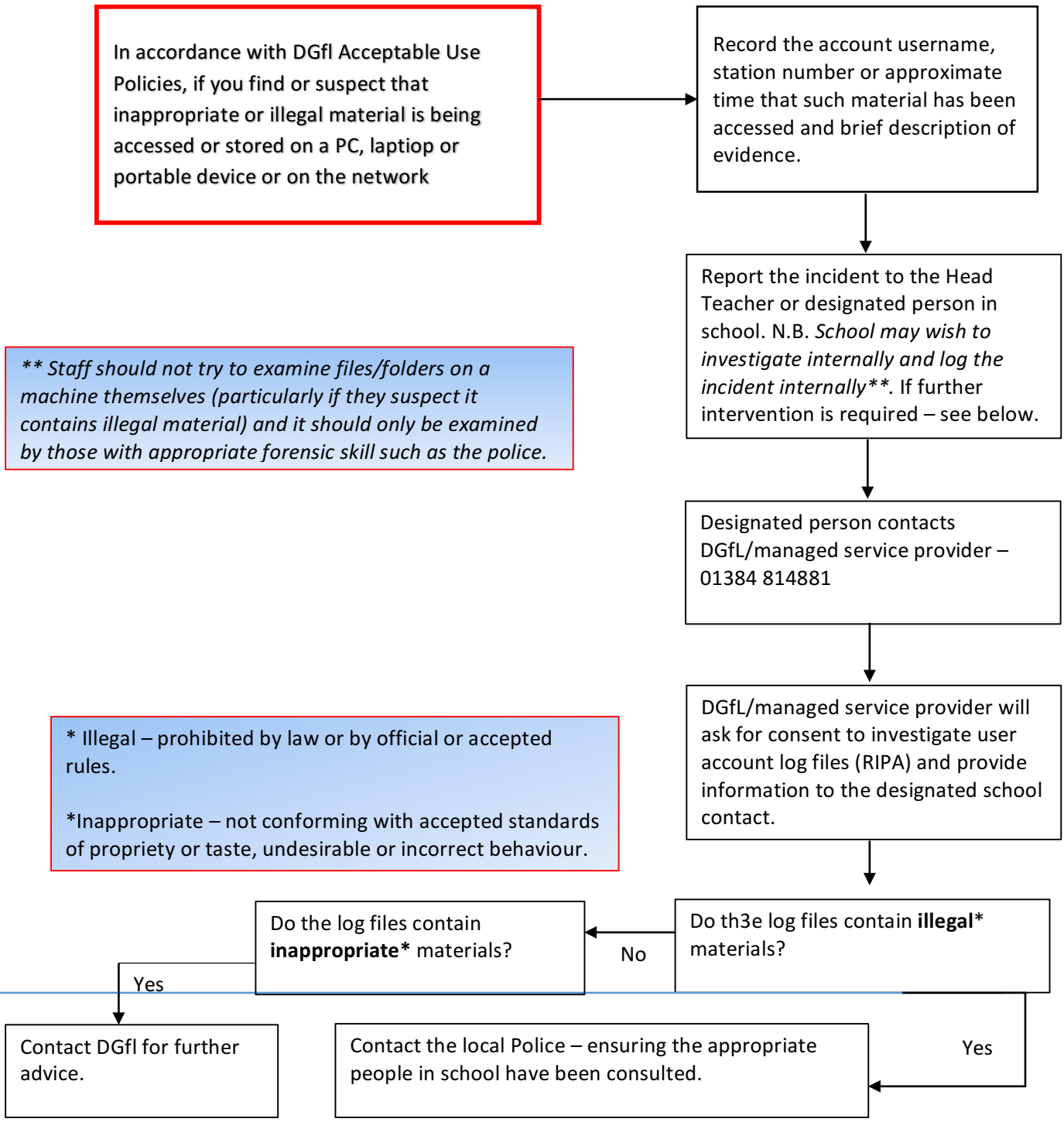
Date for review: October 2016

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

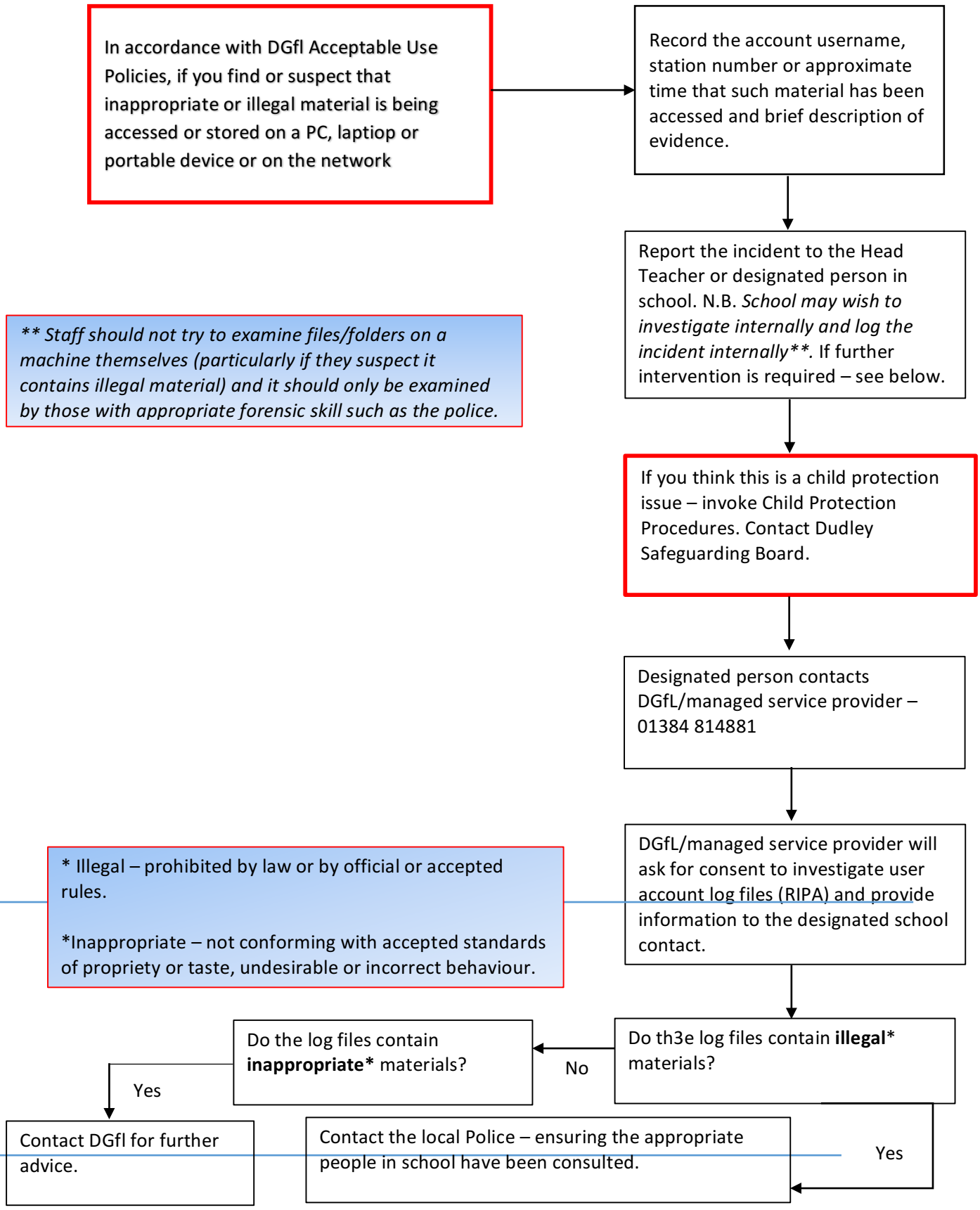
Appendix 1

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 school's 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 school's 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 school's 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
Guest Acceptable Use Policy

Visitors working in school need to sign and adhere to the following Guest AUP:

As a visitor to the school I recognise that it is my responsibility to follow school online safety advice and that I have a responsibility to ask if I am not sure of a procedure.

This is not an exhaustive list and all visitors are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

1. I understand that Information Systems and ICT include not only the school's computers, but also any personally owned equipment such as a phone or tablet and its use on social media such as Facebook or Instagram.
2. Mobile Phones will never be used for any reason when on site
3. Pupils and their families have a reasonable expectation of privacy so I confirm that I will not publish or share any information I have obtained whilst working in the school on any personal website, blog, social networking site or through any other means, unless I have written permission from the Headteacher.
4. I will not communicate with pupils or ex-pupils under the age of 18 using social media without the express written permission of the Headteacher
5. I will not give my personal contact details such as email address, mobile phone number, IM account details to any pupil or parent in the school. Contact will always be through a school approved route.
6. While in the school my use of ICT and information systems will always be compatible with the ethos of the school, and if I am in any doubt I will check this with a member of staff.
7. I understand that I have a duty of care to ensure that students in school use all forms of electronic equipment and devices safely and will report any inappropriate usage to a senior member of staff.
8. Visitors are requested not to contact a parent of a child directly, but to go through the school's official channels.
9. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.