INDIAN QUEENS COMMUNITY PRIMARY SCHOOL

E- Safety Policy

This e-safety policy was approved by the Governing Body on:	**4 November 2015**
The implementation of this e-safety policy will be monitored through:	**Monthly ICT Meetings** **Subsequent Governors' Meetings (if new recommendations / issues arise)**
Monitoring will take place at regular intervals:	**Ongoing review through monthly ICT meetings** **Full review following any new recommendations and annually Autumn Term 1st half to agree update and renewal of policy**
The Governing Body will receive a report to Governing Body on the E-Safety Policy and procedures including anonymous details of e-safety incidents:	**Governors' Meetings in Safeguarding item as appropriate (*always* Gov body Mtg (2) Autumn Term)**
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	**LA ICT Team, LA Safeguarding Unit, SWGfL, Police Commissioner's Office**

The school will monitor the impact of the policy using:

- Logs of reported incidents (through ICT meetings; ICT co-ordinator)
- SWGfL monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - pupils (eg CEOP ThinkUknow survey)
  - parents / carers
  - staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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 roles and responsibilities for e-safety 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, currently the Chair of Governors has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the Head / ICT Governor following ICT meetings
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

Headteacher / Leadership Team

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be shared with the ICT co-ordinator and technician.
- The Headteacher / Leadership Team are responsible for ensuring that the ICT co-ordinator / technician / governor and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher / Leadership Team 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 monthly ICT meeting has e-safety and training as a regular agenda item within which the monitoring and support for relevant staff will be reviewed.
- The Leadership Team will be included in the regular monitoring reports provided to the governors.
- The Headteacher and Deputy Headteacher are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see SWGfL flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)

E-Safety Co-ordinator / DCPO

- ensures that this policy and its procedures are reviewed regularly at the monthly ICT technician meetings & ICT curriculum meetings
- 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 / advises on training and advice for staff
- liaises with the Local Authority / SWGfL / LCSB
- liaises with school ICT technical and office staff, specifically the School Business Manager
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments, (for log sheets see SWGfL Safety and Security Booklet, along with the Internet Safety Protocol)
- meets regularly at the ICT meetings which includes the E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors (typically the E-Safety Co-ordinator/DSPO)
- reports regularly to the Leadership Team

  (Any incidents will be dealt with following consultation between the E-Safety Coordinator/DCPO and the E-Safety Governor, the LA Safeguarding Team and other relevant bodies. Each incident will be dealt with on an individual basis, with the aim of redressing any errors and preventing a reoccurrence. Incidents involving staff who have acknowledged the requirements of the e-safety procedures may be subject to disciplinary proceedings.)

ICT Co-ordinator / PrimaryPCSolutions (where appropriate)

The ICT Coordinator / Primary /PC Solutions are jointly responsible for ensuring that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed (as far as is reasonably practical)
- SWGfL is informed of issues relating to the filtering applied by the Grid

- the school's filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Filtering Policy Template" for good practice document)
- up to date e-safety technical information is shared with the ICT team in order that the team can effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Headteacher / E-Safety Co-ordinator for investigation
- that monitoring software / systems are implemented and updated as agreed in school policies
- ensuring effective liaison and communication with the Headteacher at all times

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 school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher / ICT Co-ordinator for investigation / action / sanction
- digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level at all times and never on a personal or informal basis
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- 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 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

Designated Child Protection Officer (who is also the E-Safety Officer)

The DCPO is trained in e-safety issues and 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

ICT Team (which is also the E-Safety Committee)

Members of the ICT / E-safety team will assist the E-Safety Officer (or other relevant person, as above) with:

- the production / review / monitoring of the school e-safety policy / documents.
- the production / review / monitoring of the school filtering policy currently provided via SWGfL

Pupils **(dependant on ability, age and maturity):**

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy (full version or summary version as appropriate regarding ability and maturity), which all pupils will agree and sign up to as a class document at the start of each school year (new pupils on arrival)
- 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 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through *home/school review meetings, newsletters, website and information about national / local e-safety campaigns / literature.*

Community Users

Community Users who access school ICT systems will be expected to sign a Community User AUP before being provided with access to school systems.

E-safety Policy Statement

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 education will be provided in the following ways:

- A planned e-safety programme (outline timetable of aspects included within e-safety) that is be provided as part of ICT / PHSCE / other lessons and is regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages are part of a planned programme of assemblies and tutorial / pastoral activities
- 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
- Pupils are helped to understand the need for the pupil acceptable user policy and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- 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 and a reminder that all are expected to follow them are displayed on log-on screens
- Staff are expected to act as good role models in their use of ICT, the internet and mobile devices

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 experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

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

- *Newsletters*
- *Parents evening, including Home/School Review Meetings*
- *Reference to the SWGfL Safe website (n.b. the SWGfL "Golden Rules" for parents) with a link on the school website*

Education – Staff

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 is available to staff. An audit of the e-safety training needs of all staff will be carried out regularly, including through 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, with the support and guidance of the ICT team members, receives regular updates through attendance at SWGfL / LA / other information / training sessions (as available) and by reviewing guidance documents released by BECTA / SWGfL / LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / whole school staff meetings and other training opportunities such as INSET / Cluster training days.
- The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training as required to individuals as required

Education – Governors

- Governors have the opportunity through their own training programme to take part in e-safety training / awareness sessions. Governors are also informed of specific training provided for pupils and welcome to attend these.
- Governors have the opportunity to attend training provided by the Local Authority / National Governors Association / SWGfL or other relevant organisation.
- Participation in school training / information sessions for staff or parents

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 ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- 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. Details of the access rights available to groups of users will be recorded by the ICT technician and will be reviewed, at least annually, by the ICT team.
- All users (at KS2 and above) will be provided with a username and password by (insert name or title) who will keep an up to date record of users and their usernames. Staff users will be required to change their password every month. Pupils currently use class log-ins in order to access relevant software programs. The school is 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. Use by pupils in this way **MUST**, therefore, ***always*** be supervised and members of staff should never use a class log on for their own network access. The school will also consider the implications of the development of Learning Platforms and home access on whole class log-ins and passwords.
- The "administrator" passwords for the school ICT system, used by the ICT coordinator / technician / Primary PC Solutions is also be available to the Headteacher / ICT governor / School Business Manager for use on a need to know basis only. A secure system is in place for access to the administrator password in an emergency.
- Users will be made responsible for the security of their username and password, must **never** 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 SWGfL
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher / ICT Coordinator.
- Any filtering issues should be reported immediately to SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the ICT Coordinator / ICT Governor / Headteacher (preferably together) – to ensure protection for these staff should any issues arise re unfiltered access. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the ICT Team (the E-Safety Committee)
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy. The monitoring and records to be reviewed and discussed at the monthly ICT meetings.
- Remote management tools are used by staff to control workstations and view users' activity but only after the staff in question have been approved by the ICT team
- All users are expected to report any actual / potential e-safety incident, IN WRITING, via email to the the ICT Coordinator / ICT Governor / Headteacher.
- 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 policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.
- An agreed policy is clearly stated in staff/community/visitor Acceptable Use Policy regarding the downloading of executable files by users

- An agreed policy is in place regarding the extent of personal use that users (staff / pupils) and their family members are allowed on laptops and other portable devices that may be used out of school. An agreed policy is in place regarding the installation programs on school workstations / portable devices
- An agreed policy 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 can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- *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, eg using search engines, 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, 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 (and other relevant 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.*
- *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.*

Use of digital and video images - Photographic, Video

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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 eg on social networking sites.**
- *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 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.*
- *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 will be obtained before photographs of pupils are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the year*
- *Student's / Pupil's work can only be published with the permission of the student / 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.

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, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (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 (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.

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 pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- 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 pupils or parents / carers (email, chat, 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.
- Whole class email addresses will be used by both KS1 and KS2 pupils.
- *Pupils are taught about email safety issues, such as the risks attached to the use of personal details. They are also taught strategies to deal with inappropriate emails and are reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.*
- *Personal information is not to be posted on the school website. Communications (other than internal / agreed emails) should be via the secretary@ email address.*

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 certain internet usage as follows:

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 any inappropriate material. The school's digital technology resources and systems will only be used for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.

Responding to incidents of misuse

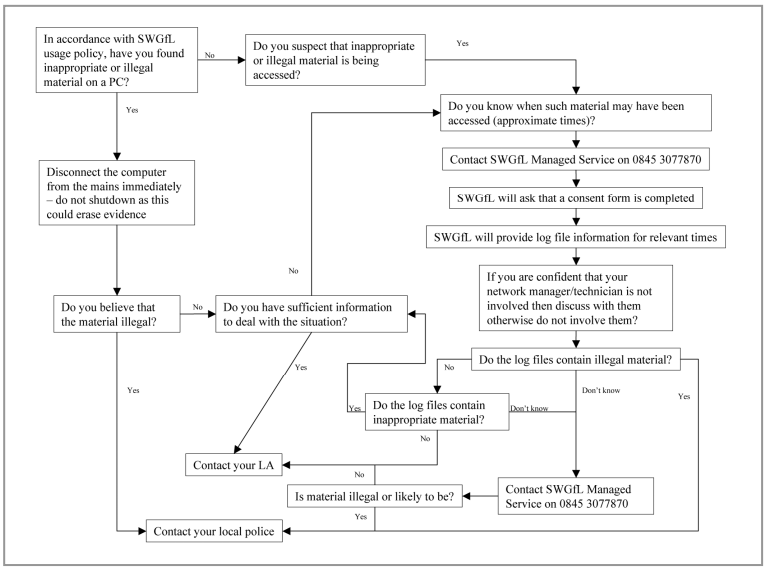
It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act

- criminally racist material
- other criminal conduct, activity or materials

The SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

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. A clear acceptable use policy is in place for all children and they are aware of its contents and any appropriate sanctions.

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School E-Safety Policy Template:

- Members of the SWGfL E-Safety Group and the SWGfL E-Safety Conference Planning Group
- Avon and Somerset Police
- Somerset County Council
- Plymouth City Council
- Swindon Borough Council
- Poole Borough Council
- Bournemouth Borough Council
- North Somerset Council
- Gloucestershire County Council
- DCSF
- Becta
- National Education Network (NEN)
- London Grid for Learning
- Kent County Council
- Northern Grid for Learning
- Bracknell Forest Borough Council
- Byron Review – Children and New Technology – "Safer Children in a Digital World"

Appendices (see separately):

- Student / Pupil Acceptable Usage Policy Proforma (2 – for younger and older pupils)
- Staff and Volunteers Acceptable Usage Policy Proforma
- Community and Student Acceptable Usage Policy Proforma