'Flying High'
Working Together to Build a Successful Future for All

E Safety Policy

Updated February 2016

Working together to build a successful future for all

Our multicultural school values and promotes a happy, safe and caring environment that is committed to helping all children experience success, whatever their background or abilities, and to ensure they achieve the highest standards in all they set out to do. The health, safety and well being of every child is our paramount concern.
This policy 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.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students / 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:

Head teacher and Senior Leaders:

- The Head teacher 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 delegated to the ICT Leader and ICT Team
- The Head teacher / Senior Leaders are responsible for ensuring that the ICT Leader and ICT Team 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 Head teacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the ICT Leader and ICT Team
- The Head teacher and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff.

ICT Leader

- leads on e-Safety
- takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
- provides training and advice for staff
- liaises with SCE
- liaises with school ICT technical staff
- receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments
- meets with SGC member to discuss current issues, review incident logs and filtering / change control logs

- reports regularly to Senior Leadership Team

School Network Manager supported by SCE Technical support staff
These staff are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the school's networks through a properly enforced password protection policy
- the school's filtering policy is applied and updated on a regular basis
- that he / she keeps up to date with e-Safety technical information in order to effectively carry out their e-Safety role and to inform and update others as relevant
- that monitoring software / systems are implemented and updated as agreed in school policies
- that if monitoring of electronic communication is to take place staff are informed in advance.

Teaching and Support Staff
are responsible for ensuring that:

- they have read and understood JSP 740 MOD Acceptable Use Policy.

they have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices

- they have read and understood the E-safety Policy and related documents.
- they report any suspected misuse or problem to the appropriate person for investigation
- digital communications with students / pupils (e-mail / Virtual Learning Environment (VLE) / voice / VTC / MOVI) should be on a professional level and only carried out using official school communication 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 an 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

Designated senior person for child protection
should be trained in e-Safety issues and be 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:

- 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
- 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

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, website / VLE and information about national / local e-Safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil ICT Code of Conduct and Acceptable Use Policy
- accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

Policy Statements

Education – students/pupils

- A planned e-Safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in and beyond school
- Key e-Safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students / 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
- Students / pupils should be helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school
- Students / pupils should be 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 will be posted in all rooms
- Staff should act as good role models in their use of ICT, the Internet and mobile devices

Education & Training – 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:

- All staff to have read and understood JSP 740.
- A planned programme of formal e-Safety training will be made available to staff. An audit of the e-Safety training needs of all staff will be 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 should receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-Safety policy and Acceptable Use Policies
- E-Safety policy will be presented to and discussed by staff in staff / team meetings / INSET days.

Training – SGC

- SGC should be aware of e-Safety and how this is applied and implemented in school
- SGC should be invited to take part in e-Safety training / awareness sessions

Technical – infrastructure / equipment, filtering and monitoring
SCE Technical Support Officer/school network manager 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 are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-Safety responsibilities.

- 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 (at KS2 and above) will be provided with a username and password
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader
- Users will be made responsible for the security of their username and password, 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 has provided appropriate user-level filtering through the use of the filtering programme.
- 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 ICT Leader, SLT or Headteacher.
- Requests from staff for sites to be added or removed from the filtered list will be actioned by the Network Manager
- 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.
- 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.
- All programs are to be sent to HQ SCE for testing before being installed on computers.
- Sensitive data is to be kept on an encrypted memory stick.
- 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.

Use of digital and video images - Photographic, Video
- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are not participating in activities that put them at risk or 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 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 students / 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

Staff must ensure that they:

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

- Users need to be aware that email communications are not secure and can be monitored
- Users must immediately report, to the nominated person, 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

In the event of inappropriate use by staff

If a member of staff is believed to misuse the Internet, VLE or cLc in an abusive or illegal manner, a report must be made to the Headteacher immediately and then the Allegations against staff Procedure and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Allegations are defined as information relating to either potential criminal conduct or conduct raising concerns about a person's suitability.

In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

In the event of inappropriate use by pupils

Should a pupil be found to misuse the on-line facilities whilst at school, through the cLc or VLE or in a setting the following consequences will occur

- Any child found to be wilfully misusing the Internet by not following the Acceptable Use Rules will have their parents called into school to discuss their child's behaviour.
- Further misuse of the rules will result in not being allowed to access the Internet for a period of time and another letter will be sent home to parents/carers.

In the event that a child or young person accidentally accesses inappropriate materials the child will report this to an adult immediately and take appropriate action to hide the screen or close the window, e.g. use 'Hector Protector', for example, (dependent on age) so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. This button is easily identifiable on the SCE cLc and the Hornbill School website. The issue of a child or young person deliberately misusing on-line technologies should also be addressed by the establishment.

Children should be taught and encouraged to consider the implications for misusing the Internet and posting inappropriate materials to websites, for example, as this can lead to legal implications.

Social Networking

The widespread availability and use of social networking applications bring opportunities to understand, engage and communicate with our audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our services users and partners, our legal responsibilities and our reputation.

For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

The requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice.

Social networking applications include, but are not limited to:

- Blogs
- Online discussion forums
- Collaborative spaces
- Media sharing services e.g. Youtube
- 'Micro-blogging' applications e.g. Twitter

Many of the principles of this policy also apply to other types of online presence such as virtual worlds and RSS aggregation services and the use of these services should also be discussed with the Communications Officer first.

All employees should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the SCE Equality and Diversity Policy.

Enforcement

Any breach of the terms set out below could result in the application or offending content being removed in accordance with the published complaints procedure and the publishing rights of the responsible Council representative being suspended.

The Agency reserves the right to require the closure of any applications or removal of content published by Agency representatives which may adversely affect the reputation of the SCE or put it at risk of legal action.

Any communications or content you publish that causes damage to the Agency, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the Agency's Dismissal and Disciplinary Policies apply.

Terms of Use

All proposals for using social networking applications as part of SCE (whether they are hosted by the Agency or by a third party) must be approved by the Communications Officer first (info@sceschools.com)

All Staff must adhere to these Terms of Use. The Terms of Use below apply to all uses of social networking applications by all staff. This includes, but is not limited to, public-facing applications such as open discussion forums and internally-facing uses such as project blogs regardless of whether they are hosted

on corporate networks or not.

SCE expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Social networking applications

- must 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 SCE into disrepute.
- must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns.
- must not be used in an abusive or hateful manner
- must not be used for actions that would put SCE staff in breach of the SCE codes of conduct.
- must not breach SCE's misconduct, equal opportunities or bullying and harassment policies.

Where individuals from partner organisations are involved and are acting on behalf of SCE, they will also be expected to comply with the relevant policies.

5.4 It is also important to ensure that members of the public and other users of online services know when a social networking application is being used for official purposes. To assist with this, all SCE staff must adhere to the following requirements:

- They must only use @sceschools.com email for user accounts which will be used for official purposes;
- Where social networking applications are being managed by SCE Staff, appropriate feedback and complaints information must be published in a prominent place which is easily accessible to other users.
- The use of the SCE logo and other branding elements should be used where appropriate to indicate SCE's support. The logo should not be used on social networking applications which are unrelated to or are not representative of the Agency's official position. Requests to use the SCE logo must be made to the aforementioned Communications Officer
- Staff should ensure that any contributions they make are professional and uphold the reputation of SCE.
- Staff must not promote or comment on political matters or issues that may be regarded as such.