E-SAFETY AND ACCEPTABLE USE POLICY

02/10/2017

Purpose

The Acceptable Use Policy (AUP) sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all technologies, particularly those on-line, (including the Internet, E-mail, web cams, Instant Messaging and other social networking spaces, mobile phones, portable media, such as memory sticks and laptops, and games) to safeguard adults and children within the school setting. It also details how Scott will provide support and guidance to, children, staff, parents/carers and the wider community (where appropriate) for the safe and responsible use of these technologies, beyond the school setting. In addition, it explains procedures for unacceptable or mis-use of these technologies by adults or children.

The use of the Internet as a tool to develop learning and understanding has become an integral part of school and home life. There will always be risks to using any form of communication which lies within the public domain therefore it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children use these technologies.

These risks include:

- Commercial issues with spam and other inappropriate e-mail.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the Internet or any mobile device.
- Viruses.
- Cyber-bullying.
- On-line content which is abusive or pornographic.

It is also important that all adults are clear about the procedures, for example, only contacting children and young people about homework via a school e-mail address, not a personal one, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

Whilst Scott acknowledges that we will endeavour to safeguard against all risks we may never be able to completely eliminate them. Any incidents that may arise will be dealt with quickly and according to policy to ensure children and young people are continued to be protected.

As part of the agenda set out by the government, the Education Act 2004 and the Children's Act, it is the duty of schools to ensure that children and young people are protected from potential harm both within and beyond the school environment. Therefore, the involvement of children and young people and parent/carers is also vital to the successful use of on-line technologies, so this policy also aims to inform how parents/carers and children or young people are part of the procedures and how children and young people are educated to be safe and responsible users so that they can make good judgements about what they see, find and use. The term 'e-safety' is used to encompass the safe use of all on-line technologies in order to protect children, young people and adults from potential and known risks.

Aims

To ensure the safeguarding of all children within and beyond the school setting by detailing appropriate and acceptable use of all on-line technologies.

- To outline the roles and responsibilities of everyone in the school community.
- To ensure adults and children are clear about procedures for misuse of any on-line technologies both within and beyond the school setting.
- To develop links with children, parents/carers and the wider community ensuring input into policies and procedures with continued awareness of benefits and potential issues of on-line technologies.

Teaching and Learning and Appropriate Use

Appropriate use by staff or adults
Staff members have access to the network so that they can access age appropriate resources for their classes and create folders for saving and managing resources. They have a password to access a filtered Internet service and know that this should not be disclosed to anyone and they should not leave a computer or other device unattended whilst they are logged in.

All staff will receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Rules, which will need to be signed and will be kept under file. The Acceptable Use Rules will be displayed prominently around the school as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

When accessing any aspects of the School website from home, the same Acceptable Use Rules will apply.

In the event of inappropriate use
If a member of staff is believed to misuse the Internet in an abusive or illegal manner, a report must be made to the Headteacher immediately and then the complaints procedure and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted, e.g. LADO.
In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

Appropriate use by children and young people
Acceptable Use Rules and the letter for children and young people and parents/carers are outlined in the Appendices and detail how children and young people are expected to use the Internet and other technologies within school or other settings, which includes downloading or printing of any materials. The rules are there for children and young people to understand what is expected of their behaviour and attitude when using the Internet which then enables them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

We want our parents/carers to support our rules with their child or young person, which is shown by signing the E-Safety Rules together so that it is clear to the school, the rules are accepted by the child or young person with the support of the parent/carer. This is carried out at the beginning of every academic year. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school. Children are reminded of the acceptable rules of e-safety each term.
If parents request any help we will assist where possible and direct them to informative websites such as 'KnowITAll for Parents' and 'CEOP'.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

In the event that a child or young person accidentally accesses inappropriate materials or displays an image or text that is not appropriate the child will report this to an adult immediately and take appropriate action to hide the screen (using the Shield) or close the window. All children will be taught explicitly how to do this.
The Computer should remain locked during the remainder of the lesson & should only be unlocked and reviewed when children have been removed from the class. The E=Saftey/ICT Leader, ICT Link governor and the Headteacher should be informed and the incident should be logged.
We adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have accidentally accessed something.

In the event of inappropriate use
How will infringements be handled? *When a student or staff member infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of the Head Teacher. The following are provided as exemplification only:*

Students

1. **Category A infringements**

- Use of non-educational sites during lessons
- Unauthorised use of email
- Use of unauthorised instant messaging/social networking sites
- ***(Possible sanctions: referred to class teacher /E-Safety Co-ordinator)***

2. **Category B infringements:**

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued use of unauthorised instant messaging/chatrooms, social networking sites, News Groups
- Corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it.
- ***(Possible sanctions: referred to class teacher/E-Safety Co-ordinator/senior teacher/removal of Internet access rights for a period /contact with parent).***

3. **Category C infringement:**

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or MSN message that is regarded as offensive, harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material
- ***(Possible Sanctions: referred to Class teacher/E-Safety Co-ordinator/Head Teacher/removal of Internet and/or Learning Platform access rights for a period/contact with parents/removal of equipment).***

4. **Category D infringements:**

- Continued sending of emails or MSN messages regarded as offensive, harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Use or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute.
- ***(Possible Sanctions – referred to Head Teacher/Contact with parents/possible exclusion/removal of equipment/refer to Community Police Office/LA E-Safety Co-ordinator).***

Staff

Category A infringement (Misconduct)

- Excessive use of internet for personal activities not related to professional development eg online shopping, personal email, instant messaging etc
- Misuse of first level data security eg wrongful use of passwords
- Breaching copyright or license eg installing unlicensed software on network
- Acting in an unprofessional manner on social networking sites eg Facebook to gossip about, bully, abuse or insult others in the school community.
- To publish school information, photographs or other similar material on social networking sites without permission from the Head Teacher.
- ***(Sanction – referred to line E Safety Co-ord/Head Teacher/warning given).***

Category B (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school/Council computer hardware or software
- Any deliberate attempt to breach data protection or computer security rules
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Use or transmission of material which infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute
- ***(Sanction – referred to Headteacher/Governors and follow school disciplinary procedures;***

report to AL Personnel/Human Resources, report to Police)

E Safety - safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop and preserve any evidence
- Instigate an audit of all ICT equipment by an outside agency such as the school's ICT managed service providers – to ensure there is no risk of students accessing inappropriate materials in the school
- Identify the precise details of the material.
- If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.
- Schools are likely to involve external support agencies as part of these investigations eg an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

E-SAFETY: Child Pornography Found

In the case of child pornography being found, the member of staff should be **immediately suspended** and the Police should be called.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection Centre (CEOP): http://www.ceop.gov.uk/reporting abuse.html

INCIDENT REPORTING

It is the responsibility of all staff to report e-safety or e-security incidents to the E-Safety/ICT Co-ordinator or Headteacher so that they can be dealt with effectively and in a timely manner in order to minimise any impact on school.

The E-Safety Co-ordinator will maintain an Incident Log. This log shall capture the following information: Incident date, description of occurrence, immediate corrective action, further action, legal implications, closed date.

The Incident Log will be reviewed by the Head Teacher once per term and the risk assessment shall be updated in light of new incidents.

Procedures for report abusive content on social media sites can be found attached to the policy. These are published by NAHT and are called Appendix 2: Procedures for Reporting Abusive Content on Social Media Sites.

The curriculum and tools for Learning

Internet use

At Scott we teach our children and young people how to use the Internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding and communicating effectively in order to further learning, through ICT and/or PSHE lessons where the following concepts, skills and competencies have been taught by the time they are in Year 6:

- Internet literacy (how to navigate safely, conduct safe searches, filter relevant sites and information)
- making good judgements about websites and e-mails received
- knowledge of risks such as viruses and opening mail from a stranger
- access to resources that outline how to be safe and responsible when using any on-line technologies eg 'U Think You Know' website
- knowledge of copyright and plagiarism issues
- file-sharing and downloading illegal content
- uploading information – know what is safe to upload and not upload personal information, including photographs of themselves
- where to go for advice and how to report abuse

When appropriate in relation to e-safety we use the www.thinkuknow.co.uk resources for KS1 and KS2.

These skills and competencies are taught within the curriculum so that children and young people have the security to explore how on-line technologies can be used effectively, but in a safe and responsible manner, for example:

Personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information including:

- full name (first name is acceptable, without a photograph)
- address
- telephone number
- e-mail address
- school
- clubs attended and where
- age or DOB
- names of parents
- routes to and from school
- identifying information, e.g. I am number 8 in the Youth Football Team

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'. Parents / carers all sign a letter of consent to give permission for their child's photograph to be taken. Parents/carers should monitor the content of photographs uploaded. Any Images of children and young people will be stored on a secure school network in line with the data protection act.

Staff or adults need to ensure they consider the risks and consequences of anything they or their children and young people may post to any web or social networking sites, as inappropriate comments or images can reflect poorly on an individual and can affect future careers. Parents are all informed that they are not allowed to upload photographs of other people's children onto any social media sites.

E-mail use

As part of the KS2 curriculum children are taught different ways of communicating and using ICT to share and present information in different forms. Where appropriate children are taught about the safety aspects of e-mailing.

When at home parents/carers are encouraged to be involved with the monitoring of E-mail usage although the best approach with children and young people is to communicate about who they may be talking to and assess risks together.

Video-conferencing

Children need to ask for permission from a member of staff or adult to use this facility both in and beyond school and should only undertake video conferencing when supervised by an adult. Taking images via a web cam will follow the same procedures as taking images with a digital or video camera Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Rules.)

Photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone. When in school there is access to:

- digi blues/flip cameras
- digital cameras/web cameras
- IPads
- Laptops with webcams

The sharing of photographs via the school website or any other means on-line will only occur after permission has been given by a parent/carer which is updated annually.

Any photographs or video clips uploaded will not have a file name of a child, especially where these may be uploaded to a school website.

Photographs should only ever include the child's first name (although Child Protection Guidance states either a child's name or a photograph but not both.) If it is possible we prefer to have Group photographs rather than pictures of individual children.

Any photographs taken will not be of any compromising positions or in inappropriate clothing, e.g. swimming kit.
The photos taken will be for the parents, or for use on the school website, school documentation and displays. Back up copies are kept on the school secure network area.

Mobile phones and other technologies
The use of mobile phones or PDAs will not be allowed in our school, or on school grounds whilst in charge of children. Lockable lockers are provided for all staff/visitors and mobile phones should be kept in them during contact time with the children. The exception being for emergencies during an after school club, on a trip or residential visit where staff will use the school mobile phones, not their personal phones to make contact. Children are not permitted to bring mobile phones into school.

- **Staff members are not allowed to use their personal numbers to contact children and young people under any circumstances.**
- **Staff members are not allowed to transfer any school information relating to children to their own personal e-mail account or to pass this information to a third party. In addition, they must not issue their personal e-mail address to parents or pupils.**
- **Staff must ensure that any data that is taken offsite must be stored on an encrypted memory device.**

Filtering and safeguarding measures

The school uses Fortinet as it's filter system, all children's profiles whilst using any computer within the school are set at a level so that inappropriate content is filtered. **All** filtering should be set to 'No Access' within any setting and then controlled via:

- Portal Control (controls filtering at local site level) which controls individual access to the Internet.
- Local Control – controls access to websites and provides the option to add to a 'restricted list'.

The Headteacher should sign a disclaimer stating agreement to the filtering levels being maintained as part of the connectivity to broadband requirements from Fortinet. In the event that the site Level is not set to 'No Access', the Headteacher and Governors should write a letter to the service provider to explain how they intend to safeguard their children and young people.

Anti-virus and anti-spyware software (Windows) is used on all network and stand alone PCs or laptops and is updated on a regular basis.

A firewall ensures information about our children and young people and the school cannot be accessed by unauthorised users.

Children use a search engine that is age appropriate such as Google Schools.

Links or feeds to e-safety websites are provided.

The wireless network has an Encryption code this will help prevent hacking.

Monitoring
Teachers monitor the use of the Internet during lessons and also monitor the use of e-mails from school,
the ICT link Governor & the ICT Technician will also undertake analysis of blocked sites from the fortinet

logs.
The ICT Leader will monitor if teachers are raising the agreed e-safety awareness as part of the curriculum

---

Links to Other Policies

Complaints Policy
Please refer to the Complaints Policy for the procedures in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies which may result in an allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations should be reported to the Headteacher immediately or Chair of Governors in the event of the allegation being against the Headteacher.

The DCFS White Paper clearly states that no personal equipment belonging to staff should be used when contacting children and young people about homework or any other school issues either in or beyond school and any such action should be dealt with. We follow this information to protect our staff members from potential allegations of misconduct by a child or parent.

PSHCE
We link the teaching and learning of e-Safety with our PSHCE curriculum by ensuring that the key safety messages are the same whether children and young people are on or off line engaging with other people. We also focus on the dangers of online bullying.

Health and Safety
Please refer to the Schools/Borough Council Health and Safety guidelines and procedures for information on related topics, particularly Display Screen Equipment. Wireless technologies are not considered to be a hazard following advice from the Health Protection Agency to the Government.

External websites
In the event that a member of staff finds themselves or another adult on an external website, such as 'Rate My Teacher', as a victim, schools/settings are encouraged to report incidents to the Headteacher and unions, using the reporting procedures for monitoring.

Disciplinary Procedure for All School Based Staff
In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of on-line technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

Equal Opportunities
This policy has been written taking account of the School's Equal Opportunities Policy.

There is a commitment to inclusive practice. Inclusion is the responsibility of everyone in the school. The Special Educational Needs and Disability Act 2001 provide a revised statutory framework for inclusion. It strengthens the right of children with SEN to attend a mainstream school, unless their parents choose otherwise or if this is incompatible with "efficient education for other children" and there are no "reasonable steps" which the school and LEA can take to prevent that incompatibility. Alongside the act, the Disability Discrimination Act 2001 places new duties on schools not to treat disabled pupils less favourably than others and to make "reasonable adjustments" to ensure they are not disadvantaged. At Scott we strive to ensure that all children have access to teaching and learning that is appropriate to their needs.

Review of Policy
The school's policy will be reviewed when:

- Annually alongside the Child Protection and Safeguarding Policy.
- There has been a significant change in staffing or pupil intake.
- There has been a significant change in Government guidelines

.

S.Worrall
E-Safety/ICT Lead
Oct 2017