Sharnbrook John Gibbard Lower School

E-safety & Acceptable Use Policy

June 2015

Date agreed at Governing sub-committee:
Chair of Committee:
Chair of Governors:
Head teacher:
Date for review:

1. Rationale

The requirement to ensure that pupils, staff and all others in the school community are able to use the internet and related communications technologies appropriately and safely is part of the wider duty of care to which all who work in schools are bound. This framework of e-safety, or acceptable use policy (AUP), is to promote safe and appropriate use. As such, it should be understood in the context of other 'child protection' and 'behaviour' policies that the school already has in place as well as other existing policies in respect of its employees.

Given the range of new technologies now available to use for educational purposes and in everyday life, the intention of this evolving policy is:

- To maximize e-safety for all members of the school community
- To help everyone understand the potential risks
- To provide guidelines (including how the policy will be regulated and any sanctions) for safe and appropriate school and home use
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.

The main areas of risk for our school community can be summarised as follows:
Content

- exposure to inappropriate content, including ignoring age ratings in games
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

These areas are covered as part of the computing curriculum.

2. Aims

The AUP aims to:

- Reflect the understanding that all members of the school community have responsibilities towards themselves, towards others and towards the school and that these responsibilities are not confined to the physical location of the school.
- Enable young people to develop their own protection strategies when adult supervision and technological protection are not available
- Provide information on where to seek help and how to report incidents
- Help young people understand that they are not accountable for the actions that others may force upon them, but that there are sanctions that the school will impose if they act inappropriately when online
- Provide guidelines for staff, parents, carers and others on safe practice
- Ensure that the practice that it promotes is regularly monitored and reviewed with stakeholders
- Ensure technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety programme

3. Intended Outcomes

- To provide a secure network for the school and secure means of home/school access
- To log incidents and act accordingly
- To establish key standards and behaviour for e-safety across the school
- To co-ordinate the activities for the school related to promoting best practice in e-safety, including the publication of guidelines for pupils, staff, parents and governors
- To ensure that we adhere to e-safety issues related to new government policies affecting schools
- To monitor the school's responses to e-safety matters and act accordingly
- To have a named Senior Information Risk Officer – (SIRO) – to co-ordinate the development and implementation of e-safety policies, with clear designated responsibilities.
- To reinforce E-safety is a whole-school issue, not something that is simply the responsibility of the ICT staff; the whole school has a responsibility to promote it.

4. Implementation

The policy has been put to the school staff and ratified by the Governors. Parents are informed through the pupils' Internet safety rules (Appendix 2) which are signed by them and their children at the beginning of the school year and are displayed in all the computer areas.

Passwords

Staff and pupil passwords are kept private and only the holder or network manager can change them. All computers with restricted or protected information must be logged off when not use. Passwords are changed at risk based intervals.

Emails

It is accepted that staff may send emails and attachments to recipients outside the school. Children may only do so under the supervision and direction of their teacher. Staff should not use their personal email when contacting parents and children.

Anti-virus and anti-spam system

The school has an up to date anti-virus and anti-spam system provided by the Local Authority which is updated weekly. This is on all computers used within the school.

Internet Filter

This school has the educational filtered secure broadband connectivity through E2BN;

We use the E2BN filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;

Video Conferencing
Under the direct supervision of a member of staff children may participate in video-conferencing with other schools.

Learning platform

Uploading of information on the school's learning platform is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;

Photographs and videos uploaded to the school's learning platform will only be accessible by members of the school community;

Pupils are only able to publish and upload onto designated areas of the learning platform.

Website

The website is only updated by the website manager who monitors the content. Pupil images are never displayed with names.

Photographs and video outside of school

Photos and videos on school trips are only to be taken on school devices and must be downloaded (and deleted from the device) on to an appropriate password protected device as soon as possible after the event. At competitions and events organised by outside agencies photographs can be taken by them with permission from the parents or if group shots with no children named and limited to the stated used. Photographs of children should not be put on social media sites.

Storage of information
There are different levels of information created and stored and this is reflected in how it is stored, where it is stored and who can access it.

Sensitive (Access limited to Head and Bursar)	Restricted (Named staff only)	Protected (All in school community)	Public (Anyone)
Personal details on Simms	Any information that identifies an individual eg IEPs, reports	Routines, management information eg timetables	Website, parentmail, display

Access to all ICT systems shall be via logins and passwords. Any exception must be SIRO approved. All information storage shall be restricted to necessary users with any additional access being SIRO approved. The SIRO must maintain a record of who has access to restricted information.

Inappropriate content and language
There will be zero tolerance to the use of inappropriate content and language on any ICT equipment within our school community.

The type of language that is used in emails should be the same as that which is used in face to face situations.
Prohibited Web use:

Chat rooms/instant messaging (except that promoted by the school for educational purposes)	Newsgroups/forums (except that promoted by the school for educational purposes
Downloads of ring tones, screensavers and games (except any promoted by the school for educational purposes)	Internet peer to peer networks
Downloads of freeware, shareware, evaluation packages (except by authorized persons and in compliance with copyright law)	

The SIRO will maintain an incident log and report on its use once a year to the governing body. (Appendix 1)

Staff
The school aims to establish a clear understanding of the responsibilities of all those involved in the education of children and young people with regard to e-safety during staff training sessions. It is expected that all staff will read (and if necessary seek clarification) all school policies. Working at this school means acceptance of those policies including this AUP.

As such:

- Staff must not store protected or restricted information on the class profiles on the network.
- Staff must not allow any emails between themselves and pupils to be anything other than school business and not through the staff member's personal email.
- Staff must not have any current or former pupil as 'on line' friends whilst they are of school age. Staff must report to the SIRO any inappropriate contact from a pupil or former pupil of school age.
- During ICT lessons pupils should be made aware of the procedures for reporting accidental access to inappropriate materials.
- In any instance of deliberate misuse the SIRO must be informed and the pupil will be dealt with in accordance with the school's behaviour policy.
- The school email accounts may be used for personal use but with the knowledge that the content may be monitored by the ICT technician.
- Staff need to be aware that conducting any personal transactions on school equipment could result in residual information remaining on the hard drive which may be accessible to others. **The school cannot accept any liability for any resulting loss or damage.**
- Staff should keep to a minimum any data which is held on their school laptop and must lock it if it is left unattended (ctrl + alt + delete, lock). The security of school laptops out of school lies with the staff who, by taking them off school premises, accept responsibility for them.
- Digital images should only be taken off site on password protected devices.
- Any restricted data that is taken away from the school premises must be securely encrypted on school devices and only accessed on those devices. Restricted data must be backed up by the Network Manager on a drive specifically set up for this purpose.
- Exporting SIMS data must only be on school devices.

- Staff should follow the schools social networking guidelines (Appendix 3)
- Staff who find inappropriate material will report it directly to the SIRO.

Pupils

Pupils are encouraged not to bring in to school personally owned devices unless they have been so requested by their teacher. Any such device should be handed into the school office for safekeeping until such time as they are required or collected at the end of the school day.
The school cannot accept any responsibility for personally owned devices (e.g. laptops, USB devices, external hard drives, mobile phones and digital cameras) brought into school or taken on educational visits. If these are to be used on the school network they must first be virus checked before they are connected or used. Staff are allowed to see the images and data collected while pupil use devices at school.
The learning platform should be used as the means for accessing school information off school premises.
Pupils are made aware of the procedures for reporting accidental access to inappropriate materials. If children accidentally find inappropriate material they are to report it to their teacher who will alert the SIRO so that s/he can take steps to rectify this. Children learn of this procedure in their lessons and it is reinforced.

Sanctions

Pupils who deliberately abuse the AUP will be dealt with in line with the school's Behaviour Policy. Parents must be informed and any incident must be logged in school by the SIRO,

This policy will be reviewed within one year of its first ratification by the school Governors

5. Personal mobile devices

Personal mobile phones and mobile devices

- Mobile phones and personally-owned devices brought into school are entirely at the staff member, pupil's, parent's or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Staff members may only use their phones outside of teaching times.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Staff mobile phones and personally-owned devices will not be used in any way during lessons or formal school time.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

- All pupil mobile phones and personally-owned devices will be handed in at reception should they be brought into school.

Appendix 1: Incident log

					Date of Incident
					Description
					Immediate corrective action
					Further action
					Legal Implications

SIRO signature

Appendix 2 Pupils' Internet Safety Rules

RULES FOR ONLINE SAFETY AT JOHN GIBBARD LOWER SCHOOL

1. I will always ask the teacher before I use the Internet and will be sensible whenever I use it.
2. I will only use the Internet for schoolwork and will only use the sites my teacher has asked me to access.
3. I will not give my name, address, email or telephone number to anyone on the Internet and I will tell the teacher if anyone asks me for my name, address, email or telephone number.
4. I will **never** agree to meet someone I have spoken to on the Internet.
5. I will not download programs or bring in programs from home on a disc or memory stick.
6. I will only e-mail people my teacher has approved and the messages I send will be polite and responsible.
7. I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself.
8. I will keep my logins and passwords secret and never use anyone elses.
9. I realise that if I don't use the Internet sensibly I will not be allowed to use it.

Appendix 3 **Social Networking Guidelines**

Social networking activities conducted online outside of work, such as blogging , involvement in social networking sites such as Facebook, Instagram, Snapchat or Twitter and posting material, images or comments on sites such as You Tube can have a negative effect on an organisation's reputation or image.
These are the key principles and code of conduct that we expect of all members of staff with respect to their responsibilities in connection with the use of social networking sites.
*In the context of this policy "everyone" refers to members of staff, governors, Friends and anyone working in a voluntary capacity at the school

Key Principles

- Everyone has a responsibility to ensure that they protect the reputation of the school, and to treat colleagues and members of the school with professionalism and respect.

- It is important to protect everyone from allegations and misinterpretations which can arise from the use of social networking sites.

- Safeguarding children is a key responsibility of all members of staff and it is essential that everyone considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the school either as a paid employee or volunteer must not communicate with children via social networking.

- This policy relates to social networking outside work. Blogging and accessing social networking sites at work using school equipment is not permitted.

Things that are prohibited

- The use of the school's name, logo, or any other published material without written prior permission from the Headteacher. This applies to any published material including the internet or written documentation.

- The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.

- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.

- The posting of any images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities.

In addition to the above everyone must ensure that they:

- Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school.

- Use social networking sites responsibly and ensure that neither their personal/professional reputation, or the school's reputation is compromised by inappropriate postings.

Potential and Actual Breaches of the Code of Conduct

In instances where there has been a breach of the above Code of Conduct, the following will apply:

- Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Disciplinary Procedure. A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school's ethos and principles.

- The Governing Body will take appropriate action in order to protect the school's reputation and that of its staff, parents, governors, children and anyone else directly linked to the school.