Highlands School

E-Safety Policy

Date of Last Review	*September 2016*
Next Review Due	
Governors Committee	*Strategic Projects*

Contents

Highlands School E-Safety Policy

What is E-Safety?

The school's E-Safety Policy reflects the importance it places on the safe use of information systems and electronic communications.
E-Safety encompasses not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology

- E-Safety concerns safeguarding children and young people in the digital world.
- E-Safety emphasises learning to understand and use new technologies in a positive way.
- E-Safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online.
- E-Safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.
- E-Safety Policy reflects the importance it places on the safe use of information systems and electronic communications.

RATIONAL AND LINKS

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school E-Safety policy should help to ensure safe and appropriate use. Highlands School must demonstrate that it has provided the necessary safeguards to help ensure it has done everything that could reasonably be expected of it to manage and reduce these risks.

LINKS TO OTHER POLICIES This policy should be read in conjunction with other school policies that relate in some way to e-safety to ensure consistency and to ensure that no aspect of safeguarding children in this area is omitted.

The E-Safety policy should be reviewed in line with the following policies:

- Child Protection
- Positive Behaviour Policy including anti-bullying
- Data Protection
- Mobile Phone Policy
- Staff Code of Conduct

MONITORING AND REVIEW

All instances of unacceptable behaviour that falls within the remit of this policy should be reported using the school Incident Reporting pro-forma, and a COPY sent to the E-Safety Coordinator – Safeguarding, who is a member of the Senior Leadership Team. A summary of all such incidents will be reported to the governing body annually through a report to the Strategic Projects sub-committee of the governing body.
The policy will be reviewed bi-annually by the Strategic Projects sub-committee of the governing body.

E-Safety Policy

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

The School E-Safety Coordinators are:

- Technical ICT Strategy Manager
- Safeguarding SLT Safeguarding Lead

The Designated member of the Governing Body responsible for E-Safety is:

- Nominated Safeguarding Governor

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 has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- meeting once a year with the E-Safety Co-ordinator
- reporting to Governors Strategic Projects committee at least once a year

Headteacher and Senior Leaders

- The Headteacher has a duty of care 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 E-Safety Co-ordinators.
- The Headteacher and Senior Leaders must be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that the E-Safety Co-ordinators and all other members of staff receive suitable training to enable them to carry out their e-safety roles.
- The Senior Leadership Team (SLT) will receive once a term monitoring reports from the SLT safeguarding lead at operational meeting.

E-Safety Co-ordinators

SLT Safeguarding Lead

Is responsible for:

- taking day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents
- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- providing training and advice for staff

- liaising with the Local Authority
- liaising with school technical staff
- receiving reports of e-safety incidents and creates a log of incidents safeguarding to inform future e-safety developments
- regularly monitoring of e-safety incident logs
- meeting once a year with the E-Safety Governor to discuss current issues, review incident logs and
- filtering / change control logs
- attending Governors Strategic Projects Committee meetings
- Reporting once a term to the Senior Leadership Team operational meeting

Should be trained in e-safety issues and be aware of the potential serious safeguarding / 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

It is important to emphasise that these are safeguarding issues, not technical issues simply that the technology provides additional means for child protection issues to develop.

Strategy Manager (Technical ICT)

Is responsible for:

- liaising with school technical staff
- receiving reports of e-safety incidents and creates a log of incidents related to technical issues to inform future e-safety developments
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs

is also responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the safety technical requirements and any Local Authority E-Safety Guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that the filtering policy is applied
- that they keep 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 the use of the network / internet / Virtual Learning Environment / remote access / e-mail is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher and E-Safety Co-ordinators
- that monitoring software / systems are implemented and updated as agreed with the Headteacher

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement (AUA)
- that they report any suspected serious misuse to safeguarding lead for investigation / action / sanction
- all digital communications with students / parents / carers should be on a professional level and only carried out using school systems
- e-safety policy is adhered to in all aspects of the curriculum and other activities
- students understand and follow the e-safety and Acceptable Use Agreements
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students are guided to sites that have been checked as suitable and that processes are in place for dealing with any unsuitable material that is found in internet searches
- in all lessons where computers are available for pupil whole class use, including cover lessons, staff will use monitoring software. If this is not available then the computers will not be used

Students

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement
- 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 policies on the use of mobile devices and digital cameras
- will be expected to know and understand 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. The school will take every opportunity to help parents/carers understand these issues through parents' evenings, letters, website, VLE and information about national / local e-safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school
- access to parents' sections of the website / VLE and online student records
- their children's personal devices in the school

Training

Key Staff

The head teacher is responsible for ensuring that the E-Safety co-ordinators in school (safety and technical) receive sufficient training to fulfil that role.

Staff

In accordance with the wider safe-guarding policy in school all staff have a responsibility for ensuring the highest standards of E-Safety to allow this to happen. Training will be offered as follows:

- 3 year E-Safety training as part of the update on safe-guarding
- all new staff will receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use Agreements
- this E-Safety Policy and its updates will be presented to and discussed by staff on inset days and in meetings when required
- the E-Safety Co-ordinators and E-learning Co-ordinator will provide advice / guidance / training to individuals as required.

Governors

The safe-guarding link Governor with responsibility for E-Safety will be provided with the relevant training as required and will be expected to have access to E-Safety training as part of the 3 year training cycle provided to staff.

Parents

The school will provide parents with an E-Safety workshop on an annual basis to specific year groups.

E-Safety in the Curriculum

E-Safety within the ICT Curriculum

At Highlands the ICT department delivers an E-safety course within the Curriculum to KS3 Students that covers the following key e-safety points:

- Learning to evaluate Internet Content
  With so much information available online it is important that students learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate

- to use age-appropriate tools to search for information online

- to acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously

Social Networking

These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online

Students are taught through the ICT curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school i.e. being aware of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.

Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run with the approval of a member of staff and will be moderated by a member of staff.

Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the school. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the anti-bullying policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would
not do in person. It is made very clear to students and members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

Students are also educated on the dangers of internet grooming/sexting and child abuse. Using real life and scenario situations students are guided with making responsible

decisions while using digital equipment.

Students will be educated through the ICT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

E Safety within the Citizenship Curriculum

E-safety, specifically internet safety and sexting, is covered as part of a general unit of work on crime and safety in Year 7.

Pastoral E-Safety

There is an expectation that safeguarding in all of its forms is addressed at whole school level through tutor time activities and assemblies or externally via performances from outside agencies (arranged by HOY).

Acceptable Use of ICT

All members of our community will be expected to read and sign the appropriate acceptable use agreement on joining the school:

Highlands School Acceptable Use Agreement: Students

Only members of the 6th form will be able to use the school WIFI for connecting their personal laptops / mobile devices to access the school's internet connection. Guest logins will be provided for onetime use for other students as requested by staff.

- I will only use ICT systems in school, including the internet, email, digital video, and mobile technologies for school purposes
- I will not download or install software on school Computers / Mobile Devices
- I will only log on to the school network, other systems and resources with my own user name and password
- I will follow the school's ICT security system and not reveal my passwords to anyone.
- I will only use my school email address to communicate with members of the school
- I will make sure that all ICT communications with pupils, teachers or others is responsible and sensible
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use
- I will only use my phone / mobile device during break times, lunch times and after school finishes, or in lessons at the direction of my teacher (in line with the school Mobile Phone Policy)
- I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher
- I will only use school ICT systems to do school work and accessing media to print
- I will not access or use school ICT systems for social media, online gaming, pornography, sexting, radicalization, self-harm or for any other purpose prohibited in this policy
- I am aware that when I take images of pupils and/ or staff, I will seek permission from them first. I must only store and use these images for school purposes and will never distribute these outside the school network without the permission of all parties involved. This includes school breaks and all occasions when I am in school uniform or when otherwise representing the school
- Only members of the 6th form will be able to use the school WIFI for connecting their personal laptops / mobile devices to access the school's internet connection. Guest logins will be provided for onetime use for other students as requested by staff.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts
- I will support the school approach to e-safety and not upload or add any images, video, sounds or text that could upset any member of the school

- I will respect the privacy and ownership of others' work on-line at all times
- I will not attempt to bypass the internet filtering system
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted
- I will adhere to any specific rules displayed for use of ICT in the library

Dear Parent/ Carer

ICT including the internet, email, mobile technologies and online resources have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of e-safety and know how to stay safe when using any ICT.

Pupils are expected to read and discuss this agreement with their parent/ carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with Deputy Headteacher Pastoral Care

Please return the bottom section of this form which will be kept on record at the school

We have discussed this document with…….. (child's name) and we agree to follow the Acceptable Use Agreement and to support the safe use of ICT at Highlands School.

Parent/ Carer Signature ……..……

Pupil Signature……..

Tutor Group …….. Date ……

Highlands School Acceptable Use Agreement: Staff, Governors and Visitors

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head teacher

- I will only use the school's email / Internet / Learning Platform (FROG) and any related technologies for professional purposes or for uses deemed acceptable by the Head teacher
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils. Exceptions can be given on a case by case basis with the approval of the Head Teacher
- I will only use the approved, secure email system(s) for school business
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or encrypted memory stick available to loan from the ICT Helpdesk team
- I will not install or purchase any hardware or software for use in the school without permission of the ICT Strategy Manager. Any hardware or Software not approved will not be supported by the ICT Helpdesk.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher
- I will support the school approach to E-safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'
- I understand that all my use of the Internet and other related technologies on school equipment can be monitored and logged while on the school network and all networks outside the school. This can be made available, on request, to my Line Manager or Head teacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I will not use a personal telephone for personal calls or texting in public areas of the school between the hours of 8.30am and 3.30pm, except in the staff room and/ or offices.
- I will always use software provided on school equipment in ICT rooms for monitoring the use by pupils

User Signature

- I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment

Signature …….…… Date ……

Full Name ……..... (printed)

Job title ……

Dealing with Inappropriate Use

Responding to incidents of misuse

Illegal incidents
If there is any suspected illegal activity, or use of indecent websites (using child abuse images), then this will need to be referred to E Safety Coordinator (Safeguarding) who where appropriate will refer this to outside agencies.

Other incidents
We would expect all members of the Highlands School to be responsible users, who will read, understand and follow school policy. Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and students to remember that they are representing the school at all times and must act appropriately.

School actions and sanctions

Inappropriate use within a school context would be deemed to be anything which contravenes the Staff or Student Acceptable User Agreement. Breaches of the policy other than illegal incidents will be dealt with in line with the Positive Behaviour Policy. However, in the event that infringements of the Highlands E-Safety Policy take place, where infringement may lead to an exclusion from school, whether through being careless, irresponsible or deliberate then a number of steps must be taken. These are as follows:

- An investigation involving the E-Safety Coordinator(s)
- The investigation should be conducted using a computer which cannot be accessed by students, and if necessary can be taken off site by police. For consistency, the same computer should be used.
- The URL of any site must be recorded and screenshots taken and stored where appropriate

Following the investigation, if action is needed then it could include one of the following:

Sanctions using the Highlands Positive Behaviour Policy, including possible exclusion (see appendix 1)
Involvement by Local Authority or national / local organisations (as relevant)
Police involvement and /or action

If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

Incidents of 'grooming' behaviour
The sending of obscene materials to a child
Adult material which potentially breaches the Obscene Publications Act
Criminally racist material
Other criminal conduct, activity or material

This computer or device in question must be isolated (as best it can) in order to preserve its state. This will prevent any discrepancies in a subsequent police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

Communicating This Policy

This policy will be published on the school website, the staff shared network area, FROG and made available in printed form from the school office upon request.

Notice of any changes will be sent by email to parents, staff and students via email.

A summary of the policy will be displayed on posters around the school.

The policy will be highlighted for students through an annual E-Safety week in assemblies and tutor periods

The acceptable use agreements will be used to highlight key responsibilities

Appendix 1

Internal Exclusion

The Internal Exclusion Room is a sanction available to school which may be used as an alternative to external exclusion. It is a room designed as a sanction to Year internally excluded students to deter them from behaviour that disrupts the learning of themselves and others and is part of the Behaviour Support Team's activities, which are managed by the Behaviour Support Team Manager.

Its purpose is to

- Allow students to reflect on their behaviour;
- Catch up with their work
- Act as a deterrent

Parents are to be informed of placement in internal exclusion

It can also be used as a holding facility for students who are pending investigation into more serious incidents.

The internal exclusion room (IER) is LO2 and is situated in the MFL corridor. The room has 6 separate workstations with supervised internet access.

External Exclusions

Fixed Term

Examples of Actions That Would Normally Lead To Fixed Term Exclusion

As a school we hold that the most important right is to be secure at all times. Behaviour likely to undermine that security is consequently regarded as a serious breach of discipline. The following offences are totally unacceptable and warrant an automatic sanction, normally exclusion for a fixed period of time.

- Serious bullying (including racial or sexual harassment or homophobia, serious as recorded in the Sanctions System)
- Serious breach of E-Safety policy (serious, as recorded in the Sanction System)
- Swearing at a member of staff
- Violence towards another pupil
- Possession of illegal substances
- Deliberate damage to property
- Theft
- Actions that put the health and safety of any other member of the school community

at risk;
- Repeated disruption to teaching and learning;
- Repeated refusal to obey reasonable instructions, thus challenging and undermining the authority of staff

Permanent Exclusion

Examples of Actions That Would Normally Lead To Permanent Exclusion

- Repeated and/or serious bullying including racial or sexual harassment or homophobia (persistent as recorded in the sanctions system);
- Persistent serious breach of E-Safety Policy; (serious, as recorded in the Sanction system)
- Actual or threatened violence against a member of staff
- Actual or threatened violence against another pupil
- Sexual abuse;
- Dealing in illegal substances;
- Second offence of possession of illegal substances;
- Possessions of an item that could be used as an offensive weapon, such as a knife
- Persistent violence towards pupils;
- Actions that put the health and safety of any other member of the school community at serious risk;
- Persistent and malicious disruptive behaviour, including open defiance or refusal to conform with agreed school policies;
- Repeated breaches of the school code of conduct. These should be documented through the sanctions system and are likely to be after the student has been on a Pastoral Support Programme and there has been no improvement.

The above lists are not exhaustive and other offences may lead to exclusion.