On-line Safety and Acceptable Usage Policy

Date last reviewed	
Committee Responsible	Student Behaviour and Safety
Designated member of staff	Andrew Newton (Associate Headteacher)
Date of next review:	Pending Approval September 2018

Scope of the Policy

This policy applies to all members of the The Hollyfield School Community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school on-line and ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the 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 On-line Safety behaviour that take place out of school. Where appropriate, incident may be referred to outside agencies, including the Police and Children's services.

STATEMENT OF INTENT

The purpose of this policy (and supporting and linked policies/ documents) is to:

- set out the key principles expected of all members of the The Hollyfield School community with respect to the use of digital technologies
- safeguard and protect and educate the students and staff
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use for the whole school community
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken

- define clear structures and processes to deal with inappropriate/illegal activity whilst using digital technology [noting that these need to be cross referenced with other school policies].
- minimise the risk of misplaced or malicious allegations made against adults who work with students

Roles and Responsibilities

On-line safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school.

A whole school approach to the safe use of ICT involves creating a safe ICT learning environment which includes three main elements at The Hollyfield School:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive On-line Safety education programme for pupils, staff and parents.

Governors

Governors need to have an overview understanding of on-line safety issues and strategies at The Hollyfield School. We ensure our governors are aware of guidance on e- Safety and are updated at least annually on policy developments.

Governors will:

- ensure an On-line Safety Policy is in place, reviewed annually and is available to all stakeholders.
- ensure that there is an On-line Safety Coordinator who has received appropriate training.
- ensure that procedures for the safe use of ICT and the internet are in place and adhered to.
- hold the Headteacher and staff accountable for On-line safety.

The Headteacher

The Headteacher will:

- ensure that there is an up to date Acceptable Usage Policy (AUP) and On-Line safety Policy
- ensure that these policies are compliant , shared, monitored and updated
- designate a member of the Senior Leadership Team as On-line Safety Co-ordinator.
- be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures).
- ensure that the On-line Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- receive regular monitoring reports from the Online Safety Co-ordinator.

The On-line Safety Co-coordinator

The school **On-line safety Co-ordinator** is Andrew Newton (Associate Headteacher). He is supported by Darren Bonehill (Assistant Headteacher)

The On-Line Safety Co-ordinator will:

- ensure that the school keeps up to date with eSafety issues and guidance through liaison with the external agencies and organisations
- ensure the Headteacher, senior leadership team, Governors and staff are updated as necessary.
- take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provide training and advice for staff
- liaise with the Local Authority / relevant body
- liaise with school technical staff
- receive reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meet regularly with On-line Safety Governor to discuss current issues, review incident logs and filtering
- attend relevant meetings
- report regularly to Senior Leadership Team

Network Manager / IT Technical Staff

The Network Manager / Technical Staff /Head of Faculty and Co-ordinator for ICT / Computing will:

- ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- ensure that the school meets required online safety technical requirements and guidance of the Achieving for Children and & the Every Child Every Day Multi Academy Trust that may apply.
- ensure that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- ensure that the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix "Technical Security Policy Template").
- ensure that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- ensure that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and On-line Safety Coordinator for investigation and action.
- ensure that monitoring software are implemented and updated as agreed in school policies.

All staff

All staff are responsible for promoting and supporting safe behaviours in their classrooms and following school on-line safety procedures. Central to this is fostering a 'No Blame' culture so that students feel able to report any bullying, abuse or inappropriate materials.

All staff will:

- ensure that they have an up to date awareness of online safety matters and of the current School On-line Safety Policy and practices.
- ensure they have read, understood and signed the Staff Acceptable Use Policy (AUP).
- ensure they have read and apply the School's Twitter Protocol and the Use of Photographs document.
- ensure they report any suspected misuse or problem to the Headteacher or Online Safety Coordinator for investigation and action.
- ensure all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems.
- ensure on-line safety issues are embedded in all aspects of the curriculum and other activities
- ensure students understand and follow the Online Safety Policy and acceptable use policies
- ensure students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- ensure that they monitor the use of digital technologies, mobile devices, cameras, iPads, etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- ensure that in lessons where internet use is pre-planned students are 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 Safeguarding Lead

The Designated Safeguarding Lead should be trained in on-line safety issues and be aware of the potential for serious child protection / safeguarding 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

Students are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement (Appendix 2).

Students:

- should 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. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's 's Online 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 understand these issues through parent information evenings, parents' evenings, weekly e-bulletin, letters, website , its Learning (VLE) and information about national & local online safety campaigns & literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and it's Learning (VLE) and on-line student records
- their children's personal devices in the school (where this is allowed)

How will complaints/concerns regarding on-line safety be handled?

The On-line Safety Coordinator and the DSL act as first point of contact for any complaint.

Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy, Behaviour Policy and Relationships Policy.

Complaints related to child protection are dealt with in accordance with school/Local authority Child Protection policies and procedures.

The school will take all reasonable precautions to ensure on-line safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The academy cannot accept liability for material accessed, or any consequences of Internet access.

Staff and students are given information about infringements in use and possible Acceptable Usage and On-Line Safety Policy sanctions. Sanctions available include:

- interview/counselling by tutor / Phase Leader / on-line Safety Coordinator / Head Teacher;
- requiring a students to take an on-line safety course
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
- referral to the School's Designated Safeguarding Lead, Vicki Price (Associate Head Teacher)
- referral to the Police.
- referral to Children's Services

EDUCATION

Students - The Curriculum

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in on-line safety is therefore an essential part of the school's on-line safety provision. Children and young people need the help and support of the school to recognise and avoid on-line safety risks and build their resilience.

On-line safety should be a focus in all areas of the curriculum and staff should reinforce on-line safety messages across the curriculum. The on-line safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned on-line safety curriculum should be provided as part of Computing and Personal Development and Wellbeing (PDW), themed days and other lessons and should be regularly revisited
- Key on-line safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities (PDW time each week in form and PDW drop down periods)
- Students should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. This is in line with the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices

- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- *Parent Information evenings*
- *Curriculum Packs*
- *Home School Partnership Agreement*
- *Weekly eBulletin*
- *Letters / Emails home*
- *Its Learning (VLE)*
- *High profile events e.g. Safer Internet Day*
- *Reference to the relevant web sites E publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers (see appendix 5 for further links / resources)*

Education – The Wider Community

The school will aim to provide opportunities for local community groups/members of the community to gain from the school's on-line safety knowledge and experience. This may be offered through the following:

- *Providing family learning courses in use of new digital technologies, digital literacy and online safety*
- *On-line safety messages targeted towards grandparents and other relatives as well as parents.*
- *The school website will provide on-line safety information for the wider community*
- *Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/ voluntary groups to enhance their On-line Safety provision (possibly supporting the group in the use of Online Compass, an online safety self-review tool - www.onlinecompass.org.uk)*

Education & Training – Staff / Volunteers

It is essential that all staff receive on-line safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal on-line safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the on-line safety training needs of all staff will be carried out annually.
- All new staff should receive on- line safety training as part of their child protection induction programme, ensuring that they fully understand the school On-line Safety Policy and Acceptable Use Agreements.
- The On-line Safety Coordinator will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This On-line Safety Policy and its updates will be presented to and discussed by staff in meetings /TLCs / INSET days.
- The On-line Safety Coordinator (or other nominated person) will provide advice/guidance/ training to individuals as required.

Training – Governors

Governors should take part in on-line safety training sessions, with particular importance for those who are members of any subcommittee involved in technology and on-line safety and safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation (e.g. LGfL).
- Participation in school training and/or information sessions for staff or parents

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that its infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the network manager (or member of the IT technical team) who will keep an up to date record of users and their usernames.
- Users are responsible for the security of their username and password and will be required to change their password every half term.
- The 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 and kept in a secure place (eg school safe)

- The network manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users.

    - Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list.
    - Content lists are regularly updated and internet use is logged and regularly monitored.
    - There is a clear process in place to deal with requests for filtering changes (see appendix for more details)

- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided differentiated user-level filtering (allowing different filtering levels different groups of users – staff/students etc)
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- The Online Safety Coordinator, Head of Faculty: Computing and Network manager have access to monitoring software.
- An appropriate system is in place for users to report any actual/potential technical incident/ security breach to the relevant person ie Contact On-line Safety Coordinator or Safeguarding Lead in first instance
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place (to be described) for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's On-line Safety education programme.

- The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy (see appendix for template policy)
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data transfer/storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected

- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and students or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content.

    - These communications may only take place on official (monitored) school systems.
    - Personal email addresses, text messaging or social media must not be used for these communications.

- Students should be taught about on-line safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable/inappropriate activities

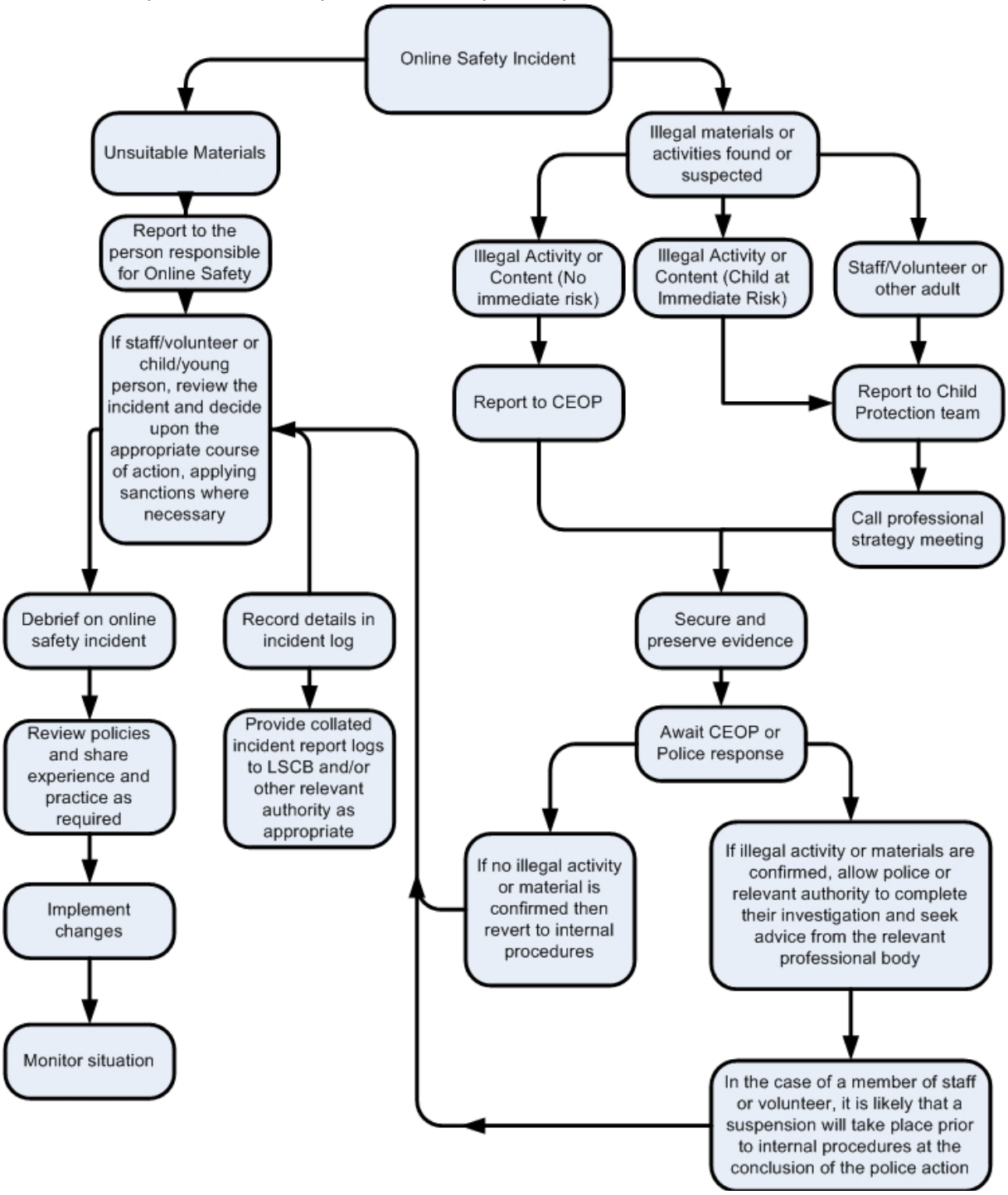
Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school/academy context, either because of the age of the users or the nature of those activities eg on-line gaming, on-line gambling.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of on-line services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is expected that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

    - Internal response or discipline procedures
    - Involvement by Local Authority Group or national / local organisation (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
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials

- Isolate the computer in question as best you can. Any change to its state may hinder a later 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 safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/ disciplinary procedures as outlined in the school Behaviour Policy.

Linked Policies and Documents

This policy should be read in conjunction with:

- Acceptable Usage Policy
- Child Protection Policy
- Preventing Extremism and Radicalisation Safeguarding Policy
- Data Protection Policy
- Allegations of Abuse Against School Staff Policy
- Behaviour Policy
- Relationships Policy
- Anti-bullying Policy
- Home & School in Partnership
- Personal Development and Wellbeing Statement
- Curriculum Pack
- Twitter Guidelines
- Use of Photographs Statement
- Staff Handbook

APPENDICES

Appendix 1: Conditions of Use of Photographs of Students

Throughout the school's academic year and your child's school life, photographs may be taken of your son/daughter.

These photographs may be used in a range of contexts:

- School publications, for example the prospectus
- School noticeboard displays
- Local newspapers as part of the media coverage of a school event
- School website
- Hollyfield School facebook , Youtube channel and twitter pages
- Internal teacher training materials and or conferences
- Local education authority publications and website.

If you do not want your son or daughter to appear in any photographs, please contact Mr A Newton as soon as possible.

Appendix 2: Acceptable Use of IT

Hollyfield School expects all students to be safe and responsible when using the internet, e-mail, social networking sites or mobile phones. In particular, students must ensure that all ICT communication is respectful and sensible. Online activity, both in and outside school, must not cause distress to others, nor bring the reputation of the school into disrepute. If students come across offensive or illegal material on line or within the schools systems, they should report this immediately to a member of staff. Students must understand that there are consequences to inappropriate or unacceptable use of ICT which could result in parents or the police being informed and/or suspension of access to their school ICT account.

Appendix 3: School Network/Internet Acceptable Usage Policy

School network

- The school network provides strictly filtered access to the internet *to support students' learning*. Student use of this service is monitored by the school. Inappropriate web sites will be blocked by the school.
- Each student is provided with a secure area on our network in which to store work. Periodic random checks will be made as to the content of these files. Students found storing inappropriate material on our network may have the facility withdrawn and action taken.
- Users will not attempt to gain unauthorised access to The The Hollyfield School Network or go beyond their authorised access. This includes attempting to log-on through another student/staff account or access another person's files. These actions are illegal, even if only for the purposes of "browsing" or "exploring".

- An individual search will be conducted if there is reasonable suspicion that users have violated this Policy. The investigation will be reasonable and related to the suspected violation.

- Users will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal.
- Storage of non-school data and applications is prohibited.

Email and Internet

- The school will issue every student with an email address which they can use both in school and at home. This is a filtered service and is programmed to automatically intercept the use of swear words and other abuse or inappropriate attachments. The school will be notified if any student abuses the email system.
- Random checks of email accounts will be made as part of our monitoring procedures and students found to be using the system inappropriately will have their accounts closed and action will be taken.
- Students who repeatedly try to access game sites, ring tone providers, chat rooms and any other sites deemed to be inappropriate by the school may have their access to the internet withdrawn.
- Any student viewing adult material will automatically have their network access withdrawn and the student's parents will be notified.
- Users will not attempt to bypass the ISP filtering system. Such attempts will result in a permanent ban of Internet access.

System Security:

- Users are responsible for their individual user area and should take all reasonable precautions to prevent others from being able to use it. Under no conditions should users let any other student know their password.
- Users will immediately notify a teacher or the system administrator if they have identified a possible security problem. Users MUST NOT go looking for security problems because this will be construed as an illegal attempt to gain access.
- Users will avoid the inadvertent spread of computer viruses. Unchecked floppy disks and USB flash/pen drives must not be used and email attachments that are suspect or from unknown sources should not be opened.
- Users will not download computer programs or files from the Internet without permission from a member of staff.
- Users will not try to load computer programs onto the The Hollyfield School Network or attempt to run programs that are not accessed through the Start Menu or Desktop screen.
- Monitoring software alerts the school to inappropriate web searches by individuals. These alerts are followed up and appropriate action is taken by the school.

Misuse of resources:

- Any student found to be tampering, damaging or otherwise abusing the School's ICT facilities will be dealt with in the strongest possible manner
- Users will avoid unnecessary printing. A record of all printing is logged automatically by the Network. Any student found to be abusing their printing quota will have their ability to print withdrawn and will be invoiced for the excessive inks and toners used
- Accessing and playing games via the Internet is not allowed. A limited number of games do have some significant educational value and these listed 'games' are the only ones users are permitted to access.

- For copyright reasons, users must not store or download commercial music of video files anywhere on the school network.
- Shared areas on the school network are for transferring files and users are responsible for their removal when they are no longer needed. If users place inappropriate files in a shared area then their network access is liable to be suspended.
- Listening to online radio broadcasts or watching website video clips online slows the whole network. Unless this is for educational reasons and permission has been given by a member of staff, this is not allowed.
- Users of iPads must not tamper with the settings or any application that has not been instructed for use. Misuse of the school's iPads is take very seriously students found to be using them inappropriately will be banned from using them and further action will be taken.

Appendix 4: Twitter Guidelines

Personal Accounts

- Personal twitter handles must not include reference to The Hollyfield School (including acronyms)
- Personal twitter accounts may not be used to tweet photos of students or student names. These must come from your department authorised accounts (listed below).
- Personal twitter accounts can be used for professional use but should include the line – All views are my own – in your bio.

- Passwords
    - Current passwords for all Social Media accounts must be held by the Network Manager (ACL) and Social Media Lead (KTE).
- Naming Students
    - DO NOT use full students' names. You may use first names, a class and a photo.
    - Full Names may only be used in the eBulletin - you may re-tweet these or send a link to articles but may not use a student's full name in a tweet.
    - If you wish to use a student's full name in a tweet; winning an award, exam success etc. Please contact the parent/guardian and seek approval on a tweet by tweet basis.
- Photographs
    - All students have been sent the updated photography consent agreement, including social media. SIMS keeps a record of all students who do not have consent to have their photos taken and staff will be given an updated list in September 2017.
    - Staff should check the no photo list before posting any images on Social Media.
- Hashstags
    - Year group hashstags are written in the format gcy followed by the year group and the year of the September they were in that year group i.e. #gcy717 should be used for the year 7s who started in September 2017.
    - If you are running a trip or activity please use a hashstag of your choice starting with gc to show Hollyfield School. This information can then be used on letters to parents etc when advertising the trips/events.
    - On the day of an event / trip please tweet @HollyfieldTweets with your hashstag.
- General tweeting guidance

- Use the School's handle (@HollyfieldTweets) to show activities / example work / anything that's happening in your classroom. You may not receive a re-tweet but your tweet will come up on the school's main feed.

Appendix 5: Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy:

UK Safer Internet Centre
Safer Internet Centre – http://saferinternet.org.uk/
South West Grid for Learning - http://swgfl.org.uk/
Childnet – http://www.childnet-int.org/
Internet Watch Foundation - https://www.iwf.org.uk/

CEOP
CEOP - http://ceop.police.uk/

Others
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis

Tools for Schools
Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

Bullying/Cyberbullying
DfE - Cyberbullying guidance -
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – new Cyberbullying guidance and toolkit (Launch spring / summer 2016) -
http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcoming-cyberbullying-work
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Social Networking
Digizen – Social Networking
UKSIC - Safety Features on Social Networks
SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people
Facebook Guide for Educators

Professional Standards/Staff Training
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs
Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
UK Safer Internet Centre Professionals Online Safety Helpline

Working with parents and carers
SWGfL Digital Literacy & Citizenship curriculum
Online Safety BOOST Presentations - parent's presentation

Connectsafely Parents Guide to Facebook
Vodafone Digital Parents Magazine
NSPCC
Get Safe Online - resources for parents
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

Appendix 6: School Technical Security Policy

(including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

RESPONSIBILITIES

The management of technical security will be the responsibility of the Network manager.

Technical Security

Policy statements

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.

- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- All users will have clearly defined access rights to school technical systems.
- Details of the access rights available to groups of users will be recorded by the Network Manager / Technical Staff (or other person) and will be reviewed, at least annually, by the Headteacher.
- Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details
- Users must report immediately any suspected breach of security.
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An agreed policy is in place (to be described) for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system.
- An agreed policy is in place (to be described) regarding the downloading of executable files and the installation of programmes on school devices by users
- An agreed policy is in place (to be described) regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on school devices. (see School Personal Data Policy Template in the appendix for further detail)
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy Template in the appendix for further detail)

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Staff Passwords

- All staff users will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames.
- the account should be "locked out" following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- should be changed at least every 60 to 90 days.
- should not re-used for 6 months.
- Staff should take care to ensure that students cannot see them logging in with passwords eg students looking over their shoulder whilst they log in.

Student Passwords

- All users will be provided with a username and password by the network manager who will keep an up to date record of users and their usernames.
- Users will be required to change their password every 60-90 days
- Students will be taught the importance of password security

Training/Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- through the Acceptable Use Agreement

Students will be made aware of the school's password policy:

- in computing lessons at the start of Year 7
- through the Acceptable Use Agreement

Audit /Monitoring /Reporting /Review

Headteacher will ensure that full records (manual or automated) are kept of:

- User Ids and requests for password changes
- User log-ins
- Security incidents related to this policy

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for on-line safety and acceptable use.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Network Manager in accordance with Department of Education Guidelines. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

Changes to the school filtering service must be authorised by the Headteacher.

All users have a responsibility to report immediately to the On-Line Safety Co-ordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon.

Education/Training/Awareness

Students will be made aware of the importance of filtering systems through the on-line safety curriculum and Acceptable Usage Policy.. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Usage Policy
- the staff handbook
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Curriculum packs which include the Acceptable Usage Policy and Use of Photographs Statements, the Home- School Agreement, the e-bulletin and through on-line safety workshops at parent information evenings