Contents

1. Introduction and overview

Creating a Safe Computing Infrastructure in School

All users of the school's computer network have clearly defined access rights, enforced using a username/password login system. Account privileges are achieved through the file/folder permissions, and are based upon each user's particular requirements – children have much more limitations in place through a standard key stage login than individual staff members do with their personal logins, for example. This helps to protect the network from accidental or malicious attempts to threaten the security of it or the data accessible using it.

Guests (e.g. supply teachers) are requested to login using a visitor login to prevent them viewing any potentially confidential data that might be stored on the schools' drives.

A permanently-enabled filtering system is provided by the local Authority, which is designed to filter out material found to be inappropriate for use in the education environment.

Access to make changes to allow or deny access to a particular website URL can be achieved by contacting the Computing co-ordinator, who will then in turn contact the local authority to do this . All changes made to Internet filtering are logged by them to help prevent abuse of the system.

Security software is installed on all *Windows* machines to prevent any malware (e.g. virus) attacks.

Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Professional conduct is essential. It is the responsibility of the user to ensure that they have logged off the system when they have completed their task and to keep their user credentials confidential to halt impersonation on the network.

Rules for Publishing Material Online (inc. Images of Pupils)

Whilst we wish the school's website to be a valuable tool for sharing information and promoting children's achievements with a global audience, we do recognise the potential for abuse that material published may attract, no matter how small this risk may be. Therefore, when considering material for publication on the website, the following principles should be borne in mind, in accordance with the school's *Child Protection Policy*:

- If an image/audio/video recording of a child is used then the relevant permissions must be checked first and they should not be named
- Files should be appropriately named in accordance with these principles
- Only images of children in suitable dress should be used and group photographs are preferred in preference to individual photographs.
- Parents are given the opportunity to withdraw permission for the school to publish images/audio/video of their child on the school website.
- Content should not infringe the intellectual property rights of others – copyright may apply to: text, images, music or video that originate from other sources. All copied or embedded content should be properly referenced.
- Content should be polite and respect others.
- Material should be proof-read

Comments submitted to posts on the website must be moderated by the post's author before being published (to ensure they are appropriate and reveal no personal information).

Children will likely use a variety of online tools for educational purposes during their time at the school. They will be asked to only use their first name or a suitable avatar for any work that will be publicly accessible and be required to follow the principles listed above before sending any work for publishing. Staff should encourage contributions that are worthwhile and develop a particular discussion topic.

When photo/videos of school events (e.g. plays) are permitted to be taken by watching parents for personal memories, they will asked not published them onto any public area of the Internet, including social networking sites.

Internet Use Contracts

Educational use of the Internet is characterised by activities that provide children with appropriate learning experiences. Clear rules which help children develop a responsible attitude to the use of the Internet have been devised. Clear expectations and rules regarding use of the Internet will be explained to all classes. A copy of the *School Pupil and Parent Acceptable Use Policy* will be given out annually at the new Reception parents' meeting and sent home to the parents/guardians of any new child who starts at Hollins Grundy. A copy is available on the school website to ensure that everybody is made aware of them.

- Pupils will need to agree to use it in a safe and responsible way, observing all of the restrictions explained to them.
- Parents will need to acknowledge that whilst the school will take reasonable precautions to prevent children from accessing inappropriate materials, the school will not ultimately be held responsible for the nature of the content they access and that they will be deemed to be accountable for their own actions.

General

Pupils are responsible for good behaviour on the Internet just as they are in a classroom or a school corridor. General school rules apply.

The Internet is provided for pupils to conduct research and communicate with others. Parents' permission is required. Remember that access is a privilege, not a right and that access requires responsibility.

Computer storage areas such as pen drives and CDs will be treated like school trays/drawers. Staff may review files and communications to insure that users are using the system responsibly. Users should not expect that files stored on servers or disks would always be private.

During school, teachers will guide pupils toward appropriate materials. Outside of school, families bear responsibility for such guidance, as they must also exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

Expectations of Pupils using the Internet

All pupils are expected to read and agree the Internet Agreement.

Pupils are only permitted to use school assigned email accounts. All email will be moderated and monitored by the class teacher. The use of unfiltered web-based email (such as Hotmail) is not permitted.Children must not to use any rude language in their email communications and contact only people they know or those the

teacher has approved. They have been taught the rules of etiquette in email and are expected to follow them.

Pupils must ask permission before accessing the Internet and have a clear idea why they are using it.

Pupils using the Internet are expected not to deliberately seek out offensive materials. Should any such material be encountered accidentally, or if any child finds themselves uncomfortable or upset by anything they discover on the Internet, they will click on The Hector's World Safety Button™ (a child-activated safety tool which children can use if something on-screen upsets or worries them) immediately and report it immediately to the supervising adult. (Any adult should report it to the Computing coordinator or Head Teacher immediately and complete an inacceptable use pro-forma). Arrangements can then be made to request that site is blocked/filtered.

Pupils' Rules for Acceptable Internet Use

- I will ask permission from a member of staff before using the Internet.
- I will respect the facilities on offer by using them safely and appropriately.
- I will not deliberately seek out inappropriate websites.
- I will report any unpleasant material to a member of staff immediately because this will help protect other pupils and myself.
- I will not download/install program files.
- I will ask permission before completing and sending forms/emails.
- I will be polite and respect others when communicating over the Internet.
- I will not give out any personal information over the Internet.
- I will not share my login details for websites with others.
- I understand that the school may check my computer files and monitor the Internet sites I visit.

Children should be encouraged to choose strong (hard to guess) passwords to ensure no unauthorised people gain access to any of their accounts.

Visitor's Rules for Acceptable Internet Use

Whilst the nature of a visitor's Internet use will clearly vary depending upon the purpose of their visit, it is still important to explain the school's expectations and rules regarding safe and appropriate Internet use to them. These differ slightly to those given to pupils to acknowledge the different situations in which visitors will likely be using the Internet:

- I will respect the facilities on offer by using them safely and appropriately.
- I will not use the Internet for: personal financial gain, political purposes, advertising, personal or private business.
- I will not deliberately seek out inappropriate websites.
- I will report any unpleasant material to a member of staff immediately because this will help protect myself and others.
- I will not download/install program files to prevent data from being corrupted and to minimise the risk of viruses.
- I will be polite and respect others when communicating over the Internet.
- I will not share my login details for websites with others.
- I will not carry out personal or unnecessary printing when using the Internet due to the high cost of ink.
- I understand that the school may check my computer files and monitor the Internet sites I visit.
- I will only access the school network via the school guest account.

An agreed process being in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the school system. All “guests” must be made aware of the staff AUP / Code of conduct and e-Safety policy.

Staff/Governor’s Rules for Acceptable Internet Use

Staff and governors are contractually obliged to use the Internet safely, appropriately and professionally within school, following the same expectations and rules as given to visitors. They are aware that they are role models for others and so should promote and model the high expected standards of behaviour at all times.

Whilst checking of personal sites (e.g. emails) is permitted outside of pupil contact time, it is recognised that this should only happen for brief periods of time and is merely a privilege (not a right) and thus can be removed at any time.

- users must immediately report any suspicion or evidence that there has been a breach of security

2. Education and Curriculum

E-Safety Education & Training

Whilst regulation and technical solutions are very important, their use must be balanced by educating users of potential e-safety risks as well as how to develop safe and responsible behaviours to minimise them, wherever and whenever they go online.
Access to the school network and internet will be controlled with regard to:

The internet feed will be controlled with regard to**:**

- the school maintaining a managed filtering service provided by an educational provider
- any filtering issues being reported immediately
- The Computing System of the school will be monitored with regard to:
- the school's technical support regularly monitoring and recording the activity of users on the school ICT systems
- e-Safety incidents being documented and reported immediately to the Computing coordinator or Headteacher or SAFEGUARDING coordinator who will arrange for these to be dealt with immediately in accordance with the AUP.

Roles and Responsibilities

Role	Responsibility
Governors	• Approve and review the effectiveness of the e-Safety Policy
Head Teacher and Senior Leaders	• Ensure that all staff receive suitable CPD to carry out their e-Safety roles • Create a culture where staff and learners feel able to report incidents • Ensure that there is a system in place for monitoring e-Safety • Follow correct procedure in the event of a serious e-Safety allegation being made against a member of staff or pupil • Inform the local authority about any serious e-Safety issues • Ensure that the school infrastructure/network is as safe and secure as possible • Ensure that policies and procedures approved within this policy are implemented

e-Safety Leader/computing coordinator	• Log, manage and inform others of e-Safety incidents • Review e-Safety policies and documents • Ensure all staff are aware of the procedures outlined in policies relating to e-Safety • Meet with Senior Leadership Team and e-Safety Governor to discuss incidents and developments • Coordinate work with the school's designated Child Protection Coordinator

Teaching and Support Staff	• Participate in any training and awareness raising sessions • • Read, understand and sign the Staff AUP • Act in accordance with the AUP and e-Safety Policy • Report any suspected misuse or problems to the e-Safety Leader • Monitor ICT activity in lessons.
Pupils	• Read, understand and sign the Pupil AUP and the agreed class internet rules • Participate in e-Safety activities, follow the AUP and report any suspected misuse • Understand that the e-Safety Policy covers actions out of school that are related to their membership of the school
Parents and Carers	• Endorse (by signature) the Pupil AUP • Discuss e-Safety issues with their child(ren) and monitor their home use of Computing systems (including mobile phones tablets and games devices) and the internet • Access the school website in accordance with the relevant school AUP • Keep up to date with issues through newsletters and other opportunities • Inform the Headteacher of any e-Safety issues that relate to the school
Technical	• Ensure the school's ICT infrastructure is as secure as possible

Support Provider	• Maintain and inform the Senior Leadership Team of issues relating to filtering • Keep up to date with e-Safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse can be reported to the e-Safety Leader/computing coordinator for investigation • Ensure monitoring systems are implemented and updated • Ensure all security updates are applied (including anti-virus and Windows)
Community Users	• Sign and follow the Guest/Staff AUP before being provided with access to school systems

2. E-Safety education

E-Safety education will be provided in the following ways:

E-Safety within the Curriculum

Early Years Foundation Stage and Key Stage 1
At this level, use of the Internet will either be quite heavily supervised or based around pre-selected, safe websites. Children will be regularly reminded about how to always take care when clicking and to seek help/advice from an adult if they see anything that makes them unhappy or that they are unsure about.

Lower Key Stage 2
Children will now be given more opportunities to develop their digital literacy skills (e.g. sending polite and friendly messages online to other children, the need to create strong passwords etc). They will be shown how to develop a responsible attitude towards searching the World Wide Web and will be reminded of the need to report any concerns they have. The importance of creating strong passwords and the benefits of only joining child-friendly websites will also be taught.

Upper Key Stage 2
Children will now be encouraged to become more independent at researching for information on the World Wide Web, being taught the necessary skills to critically evaluate sites for accuracy and suitability. They will be supported in using online collaboration tools more for communicating and sharing ideas with others, including being taught the need for not revealing personal information to strangers. The aim is to teach them how to manage and deal with risks they encounter by themselves, whilst at the same time encouraging them to become positive users of both new and emerging technologies.

Pupils are taught about how images can be manipulated in their eSafety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;

Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

E-Safety Training for Staff and Governors

Staff and governors receive regular training about how to protect and conduct themselves professionally online and to ensure that they have a good awareness of issues surrounding modern technologies, including safeguarding. They are also directed to relevant websites to help support their understanding of these issues.

E-Safety Training for Parents

The school understands that everyone has a role to play in empowering children to stay safe while they enjoy new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

For these reasons, the school provides opportunities for parents/carers to receive e-safety education and information (e.g. via the school website and during annual 'New to Year group' meetings)to enable them to better understand the issues surrounding new technologies and to help them support their children in developing good e-safety behaviour – this includes delivery via newsletters and the school website.

3 .Guidance on the use of Social Networking and messaging systems

The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.

The school recognises that many staff will actively use *Facebook*, *Twitter* and other such: social networking, blogging and messaging services, including to support their own professional development by developing personal learning networks with other educational practitioners.

Staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks – discretion and professional conduct is essential. They are encouraged to review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.

In accordance with school's Safeguarding/*Child Protection Policy/Code of Conduct*, it is never acceptable to accept a friendship request from a child from the school as in almost all cases children of primary age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends ex-pupils who are still minors to again avoid any possible misinterpretation of their motives or behaviour which could be construed as grooming.

Staff should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers. All correspondence should be via school systems.

4 .Data Protection

All data held on the school's network is subject to the *Data Protection Act 1998* and the school's *Child Protection Policy*.
At this school:

- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record

  We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

  - staff,
  - governors,
  - pupils
  - parents

- We follow LEA guidelines for the transfer of any data, such as reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- School staff and governors have access to authority approved email via Office 365 and ask that they follow the security processes required by those systems.

- Unlicensed or personal software must not be installed on the school's hardware or connected in any way to the school's equipment or systems. If software is deemed to be of use to the school then it should be duly acquired by the school under licence.

- Where data of a personal nature such as: school reports, IEPs, correspondence and assessment data is taken home on a school laptop or other portable storage media, it must be recognised that this data comes under the *Data Protection Act* and is subject to the school's *Child Protection Policy*. Care must therefore be taken to ensure its integrity and security. It should be removed from any portable device including USB pens and memory cards as soon as possible.

- Where authorisation has been given to a specific user to use a portable storage medium (e.g. memory stick) it is his/her responsibility to ensure that it does not transmit any viruses onto the school's network. It is recommended that pupils refrain from using such media unattended.

- Staff are encouraged to use the drives on the school network as a central repository for documents such as policy and planning files. Confidential pupil data may be safely stored here as access is only permissible through login by a member of school staff.

- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.
- All pupil work is stored in a folder on the network. Children's' files cannot be moved or deleted whilst logged onto a machine as a pupil user.

Data Backups

Data stored on the school's networked drives are backed up regularly so that copies of files may be recovered if the original becomes either lost or damaged.

Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory.

Details of all school-owned software will be recorded in a software inventory.

All redundant equipment will be disposed of through an authorised agency.

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

5. Equipment and Digital Content

Personal mobile phones, iPhone watches and other mobile devices

- Designated *'no mobile phone use allowed'* areas are situated in the setting, and signs to this effect are to be displayed throughout**.**
- Mobile phones/devices brought into school are entirely at the staff member, pupils & parents' 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.
- The School does not allow pupils to bring mobile phones/iPhone watches into school.
- If a pupil brings a mobile phone/iPhone watch/ mobile device is brought into school it must be turned off (not placed on silent) and stored in the office. They must remain turned off and out of sight until the end of the day.
- Staff members may use their phones during school break times, except in restricted areas .
- 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/device 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.

- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- 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.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras must be noted in school. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity, except in case of emergency. The headteacher should be informed of any such situations as soon as possible.
- Staff will be issued with a school phone where contact with pupils, parents or carers is required.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

5. Responding to Unacceptable Internet Use

Responding to Unacceptable Internet Use by Pupils

Pupils should be made aware that all e-safety concerns will be dealt with: promptly, sensitively and effectively so that they will feel able and safe to report any incidents.

Children are encouraged to respect the facilities offered to them, however staff are trained in how to proceed following a breach of the *Rules for Acceptable Internet Use*, in accordance with the school's *Safeguarding Policy*. This includes guidance on preservation of evidence and immediate reporting – the school's child protection officer has overall responsibility for Internet safety so any misuse should be reported to them without delay.

Depending on the severity and nature of the misuse offence, sanctions include: first warnings, temporary bans from using the Computing resources and meetings with parents/carers, all in accordance with the school's *Behaviour Policy* and in consideration of the age of the child.

All incidents should be recorded in the school's behaviour log book/file.

A '*report abuse'* button is visible on the E safety page of the school's website for children to click on if they are concerned about something that has happened online whilst they are on the Internet at home (e.g. cyber-bullying). This takes them to a portal to gain support and advice from the *Child Exploitation and Online Protection Agency*.

Responding to Unacceptable Internet Use by Staff and Visitors

Failure to comply with the *Rules for Responsible Internet Use* could lead to sanctions being imposed and possible disciplinary action being taken, in accordance with the school's *Safeguarding Policy*, Code of Conduct, *Child Protection Policy* and the law. Misuse should be reported without delay.

7 .Policy Review

This policy is reviewed regularly to respond to any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

The school has an e-safety coordinator who will be responsible for document ownership, review and updates.

The e-safety policy has been written by the school e-safety Coordinator/computing coordinator and is current and appropriate for its intended audience and purpose.

There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school e Safeguarding policy will be discussed in detail with all members of teaching staff.