Houldsworth Valley Primary Academy

E-SAFETY POLICY

Written: SEPTEMBER 2017

Review: SEPTEMBER 2019

Signed: **Chair of Governors**

Signed: **Headteacher**

Houldsworth Valley Primary Academy

E-SAFETY POLICY

CONTENTS

1. INTRODUCTION

1.1 Rationale

Our aim in presenting an e-safety policy is to create a safe environment where we can both work and learn. This environment should be safe for both young people and adults alike.

E-Safety is not purely a technological issue. The responsibility for e-safety must not be solely delegated to technical staff, or those with a responsibility for ICT.

Schools must therefore, firmly embed e-safety within all safeguarding policies and practices. This then makes that responsibility rest with of all those who work with young people whether in a paid or unpaid capacity.

No one policy or technology can create the safe learning and working environment we need. Schools can work towards this by combining the following:

1. Policies and Guidance.
2. Technology Based Solutions.
3. Education in terms of acceptable use and responsibility.

1.2 Policies

The policies and guidance to help form safe environments to learn and work in include, but are not limited to:

- The school Mobile phone and digital photography.
- The staff Guidance for the Safer Use of the Internet.

These policies set the boundaries of acceptable use. Schools need to use these policies however in conjunction with other policies including, but not limited to:

- The Behaviour Management Policy.
- The Anti-Bullying Charter.
- The Staff Handbook/Code of Conduct for Staff

1.3 Technology

The technologies to help form a safe environment to learn and work include:

- Internet filtering. EXA provides a system.
- Antivirus Software - regularly updated.

The policy also:

- Sets out the key principles expected of all members of the school community at Houldsworth Valley Primary Academy with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Houldsworth Valley Primary Academy.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.

- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyber bullying which are cross referenced with other school policies.
- 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.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

2. THE MAIN AREAS OF RISK FOR OUR SCHOOL COMMUNITY

2.1 Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites.
- Content validation: how to check authenticity and accuracy of online content.

2.2 Contact

- Grooming.
- Cyber bullying in all forms.
- Identity theft, including 'frape' (hacking Facebook profiles) and sharing passwords.

2.3 Conduct

- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well-being (amount of time spent online - internet or gaming).
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images).
- Copyright (little care or consideration for intellectual property and ownership - such as music and film) (Ref. Inspecting e-safety: new Ofsted Guidance 2013).

2.4 Scope

This policy applies to all members of Houldsworth Valley Primary Academy community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour policy.

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 e-safety behaviour that take place out of school.

3. KEY RESPONSIBILITIES

3.1 Headteacher

- To take overall responsibility for e-safety provision.
- To take overall responsibility for data and data security.
- To ensure the school uses an approved, filtered internet service, which complies with current statutory requirements.
- To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant.
- To be aware of procedures to be followed in the event of a serious e-safety incident.
- To receive regular monitoring reports from the e-safety co-ordinator.
- To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures.

3.2 E-Safety Lead

- To take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy.
- Promotes an awareness and commitment to e-safeguarding throughout the school community.
- Ensures that e-safety education is embedded across the curriculum.
- Liaises with ICT technical staff.
- To communicate regularly with SLT and the designated e-safety Governor to discuss current issues, review incident logs and filtering change control logs.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident.
- To ensure that an e-safety Incident Log is kept up-to-date.
- Facilitates training and advice for all staff.
- Liaises with the Local Authority and relevant agencies.
- Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
  - sharing of personal data
  - access to illegal/inappropriate materials
  - inappropriate online contact with adults/strangers
  - potential or actual incidents of grooming
  - cyber bullying and use of social media

3.3 Governors

- To ensure that the school follows all current e-safety advice to keep the children and staff safe.
- To approve the e-safety policy and review 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.
- To support the school in encouraging parents and the wider community to become engaged in e-safety activities.

The role of e-safety Governor will include:

- Regular review with the e-safety lead (including e-safety incident logs, filtering/change control logs).

3.4 PSHE/Computing Lead

- To oversee the delivery of the e-safety element of the computing curriculum.
- To liaise with the e-safety Lead regularly.

3.5 Technician

- To report any e-safety related issues that arise, to the e-safety co-ordinator.
- To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed.
- To ensure that provision exists for misuse detection and malicious attack, e.g. keeping virus protection up-to-date.
- To ensure the security of the school ICT system.
- To ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices.
- The school's policy on web-filtering is applied and updated on a regular basis.
- JSPC is informed of issues relating to filtering.
- That he/she keeps up-to-date with the school's e-safety policy and 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/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the e-safety co-ordinator/Headteacher for investigation/action/sanction.
- To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To keep up-to-date documentation of the school's e-security and technical procedures.

3.6 Administrative Lead for Data

- To ensure that all data held on pupils on the school office machines have appropriate access controls in place.

3.7 Teachers

- To embed e-safety issues in all aspects of the curriculum and other school activities.
- To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities, if relevant).
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content, such as copyright laws.

3.8 All Staff

- To read, understand and help promote the school's e-safety policy and guidance.
- To read, understand, sign and adhere to the school staff Acceptable Use/Agreement/Policy.
- To be aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices.
- To report any suspected misuse or problem to the e-safety co-ordinator.
- To maintain an awareness of current e-safety issues and guidance, e.g. through CPD.
- To model safe, responsible and professional behaviours in their own use of technology.
- To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones, etc.

3.9 Pupils

- Read, understand, sign and adhere to the Student/Pupil Acceptable Use policy (note: at KS1, it would be expected that parents/carers would sign on behalf of the pupils).
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials.
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To know and understand school policy on the use of mobile phones, digital cameras and handheld devices.
- To know and understand school policy on the taking/use of images and on cyber bullying.
- To 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.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- To help the school in the creation/review of e-safety policies.

3.10 Parents

- To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement, which includes the pupils' use of the internet and the school's use of photographic and video images.

- To read, understand and promote the school Pupil Acceptable Use Agreement with their children.
- To access the school website/Learning Platform/online student/pupil records in accordance with the relevant school Acceptable Use Agreement.
- To consult with the school if they have any concerns about their children's use of technology.

4. EXTERNAL GROUPS

Any external individual/organisation will sign an Acceptable Use policy prior to using any equipment or the internet within school.

5. COMMUNICATION

How the policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website.
- Policy to be part of school induction pack for new staff.
- Acceptable Use Agreements discussed with pupils at the start of each year.
- Acceptable Use Agreements to be issued to whole school community, usually on entry to the school.
- Acceptable Use Agreements to be held in pupil and personnel files.

6. HANDLING COMPLAINTS

The school will take all reasonable precautions to ensure e-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. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling by class teacher/e-safety lead/Headteacher.
- 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 LA/police.

Our E-Safety Co-ordinator acts 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 Bullying policy. Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.

7. REVIEW AND MONITORING

The E-Safety policy is referenced from within other school policies: Child Protection policy, Bullying policy and Behaviour policy.

- The school has an e-safety lead who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- The e-safety policy has been written by the school e-safety lead and Headteacher 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 and other stakeholders such as the PTA. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

8. EDUCATION AND CURRICULUM

8.1 Pupil E-Safety Curriculum

This school has a clear, progressive e-safety education programme as part of the computing curriculum/PSHE curriculum. It is built on national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:

- To STOP and THINK before they CLICK or Zip it, Block it, Flag it.
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To be aware that the author of a website/page may have a particular bias or purpose and to develop skills to recognise what that may be.
- To know how to narrow down or refine a search.
- For older pupils to understand how search engines work and to understand that this affects the results they see at the top of the listings.
- To understand acceptable behaviour when using an online environment email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- To understand why online ‘friends’ may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- To understand why they must not post pictures or videos of others without their permission.
- To know not to download any files, such as music files, without permission.
- To have strategies for dealing with receipt of inappropriate materials.
- For older pupils to understand why and how some people will ‘groom’ young people for sexual reasons.
- To understand the impact of cyber bullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.

- To know how to report any abuse including cyber bullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.
- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use policy, which every student will sign.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights.
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include risks in pop-ups; buying online; online gaming/gambling.

8.2 Staff and Governor Training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.
- Makes regular training available to staff on e-safety issues and the school's e-safety education program; annual updates/termly staff meetings etc.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safeguarding policy and the school's Acceptable Use policies.

8.3 Parent Awareness and Training

This school runs a rolling programme of advice, guidance and training for parents, including:

- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear.
- Information leaflets, in school newsletters, on the school website.
- Demonstrations, practical sessions held at school.
- Suggestions for safe internet use at home.
- Provision of information about national support sites for parents.
- Year 1 workshop with parents and pupils

9. EXPECTED CONDUCT

In this school, all users:

- Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use policy, which they will be expected to sign before being given access to school systems. At KS1, it would be expected that parents/carers would sign on behalf of the pupils.

- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- 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.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking/use of images and on cyber bullying.

9.1 Staff

Staff are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and handheld devices.

9.2 Pupils

Pupils should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

9.3 Parents

Parents should provide consent for pupils to use the internet, as well as other technologies, as part of the e-safety Acceptable Use Agreement form at time of their child's entry to the school. They should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

10. INCIDENT MANAGEMENT

In this school there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.

- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- Support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues.
- Monitoring and reporting of E-Safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, governors/the LA/LSCB.
- Parents/carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

11. MANAGING THE ICT INFRASTRUCTURE

11.1 Internet Access, Security (Virus Protection) and Filtering

This school:

- Has the educational filtered secure broadband connectivity through Exa.
- Uses a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status.
- Ensures network healthy through use of anti-virus software etc. and network set-up so staff and pupils cannot download executable files.
- Uses DfE and LA approved systems, secured email to send personal data over the internet (Egress) and uses encrypted devices (memory sticks) or secure remote access were staff need to access personal level data off-site.
- Blocks all Chat rooms and social networking sites except those that are part of an educational network.
- Only unblocks other external social networking sites for specific purposes/internet Literacy lessons.
- Has blocked pupil access to music download or shopping sites - except those approved for educational purposes at a regional or national level, such as Audio Network.
- Uses security time-outs on internet access where practicable/useful.
- Works to ensure any concerns about the system are communicated so that systems remain robust and protect students.
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns.
- Requires staff to preview websites before use [where not previously viewed or cached]; plans the curriculum context for internet use to match pupils' ability, using child-friendly search engines where more open internet searching is required; e.g. yahoo for kids or ask for kids, Google Safe Search.
- Never allows/is vigilant when conducting 'raw' image search with pupils, e.g. Google image search.
- Informs all users that internet use is monitored.
- Informs staff and students that that they must report any failure of the filtering systems directly to the e-safety lead.
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse - through staff meetings and teaching programme.
- Provides advice and information on reporting offensive materials, abuse/bullying etc. available for pupils, staff and parents.
- Immediately refers any material we suspect is illegal to the appropriate authorities, police and the LA.

11.2 Network Manager

This school:

- Uses individual, audited log-ins for all users.

- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
- Uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and internet websites, where useful.
- Has additional local network auditing software installed.
- Storage of all data within the school will conform to the UK data protection requirements.

Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

11.3 Ensuring the Network is Used Safely

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety policy. Following this, they are set-up with internet, email access and network access. Online access to service is through a unique, audited username and password. We also use the same username and password for access to our school's network.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes.
- Makes clear that no one should logon as another user and makes clear that pupils should never be allowed to logon or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network.
- Has setup the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- Requires all users to always log off when they have finished working or are leaving the computer unattended.
- Where a user finds a logged-on machine, we require them to always log-off and then logon again as themselves. Users needing access to secure data are timed out after 15 minutes and have to re-enter their username and password to re-enter the network.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day.
- Has setup the network so that users cannot download executable files/programmes.
- Has blocked access to music/media download or shopping sites - except those approved for educational purposes.
- Scans all mobile equipment with anti-virus/spyware before it is connected to the network.
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by site manager; equipment installed and checked by approved suppliers/LA electrical engineers.

- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role; e.g. teachers access report writing module, SEN coordinator - SEN data.
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school/LA approved systems.
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support.
- Makes clear responsibilities for the daily back up and finance systems and other important files.
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data that complies with external Audit's requirements.
- Uses the DfE secure website for all CTF files sent to other schools.
- Ensures that all pupil level data or personal data sent over the internet is encrypted or only sent within the approved secure system in our LA secure file exchange (Egress).
- Follows advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network.
- Our wireless network has been secured to industry standard Enterprise security level/appropriate standards suitable for educational use.
- All computer equipment is installed professionally and meets health and safety standards.
- Projectors are maintained so that the quality of presentation remains high.
- Reviews the school ICT systems regularly with regard to health and safety and security.

11.4 Passwords Policy

This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it.

- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use STRONG passwords.
- We require staff to change their passwords into secure systems such as emails every 90 days.

11.5 Email

This school:

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account.
- Will contact the police if one of our staff or pupils receives an email that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up-to-date.
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the police.

- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus products, plus direct email filtering for viruses, trojans, pornography, phishing and inappropriate language. Finally, and in support of these, Filtering monitors and protects our internet access to the World Wide Web.

11.6 Email: Staff

All staff sign our LA/School Agreement Form AUP to say they have read and understood the E-Safety rules, including email and we explain how any inappropriate use will be dealt with.

- Staff only use email systems for professional purposes.
- Access in school to external personal e mail accounts may be blocked.
- Never use email to transfer staff or pupil personal data. We use secure, LA/DfE approved systems including Egress.
- Staff know that email sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style'.
- The sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used.
- The sending of chain letters is not permitted.
- Embedding adverts is not allowed.

11.7 Email: Pupils

Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including email and we explain how any inappropriate use will be dealt with.

Pupils are introduced to, and use email as part of the ICT/Computing scheme of work.

Pupils are taught about the safety and 'netiquette' of using email both in school and at home, i.e. they are taught:

- Not to give out their email address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer.
- That an email is a form of publishing where the message should be clear, short and concise.
- That any email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- They must not reveal private details of themselves or others in email, such as address, telephone number etc.
- To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe.
- That they should think carefully before sending any attachments.
- Embedding adverts is not allowed.
- That they must immediately tell a teacher/responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature.
- Not to respond to malicious or threatening messages.
- Not to delete malicious of threatening emails, but to keep them as evidence of bullying.

- Not to arrange to meet anyone they meet through email without having discussed with an adult and taking a responsible adult with them.
- That forwarding 'chain' email letters is not permitted.

11.8 School Website

The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.

- Uploading of information is restricted to our website authorisers, e.g. administration officer.
- The school website complies with the statutory DfE guidelines for publications.
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the website is the school address, telephone number and we use a general email contact address. Home information or individual email identities will not be published.
- Photographs published on the web do not have full names attached.
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.
- We do not use embedded geodata in respect of stored images.
- We expect teachers using school approved blogs or wikis to password protect them and run from the school website.

11.9 Social Networking

Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

The school's preferred system for social networking will be maintained in adherence with the communications policy.

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

11.10 Video Conferencing

This school only uses approved or checked webcam sites.

12. DATA SECURITY

12.1 Management Information Systems Access/Data Transfer Strategic and Operational Practices

At this school:

- The Headteacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who is/are the key contact/s for key school information. We ensure that staff know who to report to regarding any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record in SIMS.

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

This makes clear staffs' responsibilities with regard to data security, passwords and access.

We follow LA guidelines for the transfer of any data, such as information sent to Children's Services/Family Services, Health, Welfare and Social Services.

- We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email and network access access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual housekeeping to review, remove and destroy any digital materials and documents which need no longer be stored.

12.2 Technical Solutions

Staff have secure area(s) on the network to store sensitive documents or photographs.

- We require staff to logout of systems when leaving their computer.
- We use secure sites to securely transfer CTF pupil data files to other schools.
- We use a secure VPN solution for remote access into our systems.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any back-up tapes in a secure, fireproof safe. No back-up tapes leave the site on mobile devices.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded.

13. EQUIPMENT AND DIGITAL CONTENT

13.1 Personal Mobile Phones and Mobile Devices

It is our intention to provide an environment in which children, parents and staff are safe from images being recorded inappropriately, in turn eliminating the following concerns:

- Staff being distracted from their work with children.
- The inappropriate use of mobile phone and cameras around children.

Mobile phones brought into school are entirely at the staff member, students and parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.

- Student mobile phones which are brought into school must be turned off (not placed on silent) and stored with the Reception Office on arrival at school. 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. 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. Photographs must be downloaded and wiped from the phone before the member of staff leaves the school building. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or handheld devices may be searched at any time as part of routine monitoring.
- 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.

- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- 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.

13.2 Staff Use of Personal Devices

Staff handheld devices, including mobile phones and personal cameras must be noted in school - name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted as soon as possible.

- Normal telephone communication on school business should take place using the school's telephone. Staff are not advised to use their own mobile phones or devices for contacting or responding to children, young people or their families within or outside of the setting in a professional capacity, unless there are exceptional circumstances, which have been agreed by a member of the senior leadership team.
- Staff must not give their home or mobile telephone number to pupils.
- Staff must not enter into instant messaging communications with pupils.
- Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

Staff should not use personally-owned devices, such as cameras, to take photos or videos of students and will only use work-provided equipment for this purpose. If a member of staff breaches the school policy, then disciplinary action may be taken.

- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during offsite activities, or for contacting students or parents, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes. Wherever possible, staff should contact the School Office, who will then contact parents etc.

13.3 Students Use of Personal Devices

The School strongly advises that student mobile phones should not be brought into school.

- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.

13.4 Digital Images and Video

We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school

- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.
- If specific pupil photos (not group photos) are used on the school website, in the Prospectus or in other high profile publications, the school will obtain individual parental or pupil permission for its long-term use.
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their e-safety 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 ICT 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 identity 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.

13.5 Asset Disposal

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. Further information can be found on the Environment Agency website.

- 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. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.

APPENDIX 1

Houldsworth Valley Primary Academy

STUDENT USER AGREEMENT FORM FOR THE STUDENT ACCEPTABLE USE POLICY

I agree to follow the school rules when using the school computers.

I will use the network in a sensible way and follow all the rules explained by my teacher.

I agree to report anyone not using the computers sensibly to my teacher.

I also agree to tell my teacher or another member of staff, if I see any websites that that make me feel unhappy or uncomfortable.

I will hand my mobile phone to the school office daily. (Year 5 & 6 only)

If I do not follow the rules, I understand that this may mean I might not be able to use the computers.

Student Name:

As the parent/legal guardian of the pupil named above, I give permission for my child to access networked computer services such as the Internet and e-mail. I give permission for my child to bring their mobile phone to school. I understand that the mobile phone will be left in the school office during the school day.

I understand that pupils will be held accountable for their own actions.

I also understand that although the school will take reasonable steps to ensure that my child is appropriately supervised, according to age and responsibility, I will not hold the school or County Council responsible for inappropriate material that my child may obtain.

I understand the school reserves the right to apply monitoring arrangements to any student in relation to network, e-mail and Internet use where misuse is suspected. I accept responsibility for setting standards for my son or daughter to follow when selecting, sharing and exploring information and media. I agree to report any misuse of the network to the school.

Parent/Carer/Guardian's Name:

Parent/Carer/Guardian's Signature:

Date: