



Harehills Primary School

Computing Policy Documents

September 2021

Table of Contents

Computing Policy	2
Overview	2
Aims of Computing Provision	2
Resourcing our Computing Provision	3
The Teaching of Computing	4
Planning	4
Assessment	4
Monitoring	4
Differentiation	5
Saving of Pupil Work on the Server	5
The Role of the Senior Leadership Team	6
The Role of the Computing Team	6
The Role of Subject Leaders	6
The Role of Teachers	6
Staff Development	7
Continuity and Progression in Computing	7
Pupils with Special Educational Needs	7
The Internet	7
New Equipment	8
Health and Safety	8
Policy Update	8
School Online Safety Policy	9
Writing and reviewing the online safety policy	9
Introduction	10
Relevant Legislation and Guidance	11
Unacceptable Use	11
Sanctions	13
Rationale	13
Communication	13
Online Safety	13
Responsibilities	14
Teaching and learning	15
Managing Internet Access	17
Pupils	19
Parents	20
Protection from Cyber Attacks	21
Internet Access	25
Parents and Visitors	25
Policy Decisions	27
Communications Policy	28
Staff ICT Code of Conduct	29
Acceptable Use Policy Year1/Year2	30
Acceptable Use Policy Year3/Year4/Year 5/Year 6	31

Computing Policy

Overview

ICT is changing the lives of everyone. Through teaching ICT, we equip children to participate in a rapidly-changing world where work and leisure activities are increasingly transformed by technology. We enable them to find, explore, analyse, exchange and present information. We also focus on developing the skills necessary for children to be able to use information in a discriminating and effective way. ICT skills are a major factor in enabling children to be confident, creative and independent learners. ICT also facilitates us to be able to be more effective teachers. Personalising learning is critical to the next generation of education, and with this in mind, our ICT Policy has been refocused on how we can personalise our *children's learning and give* them the opportunities to develop their own skills at their own pace. The focus on the new curriculum is now on Computing, rather than ICT as a whole. This has meant that the new curriculum is vastly different to the old curriculum.

The aims of the current ICT Provision

The aims of ICT within our school are to enable children:

- To provide pupils with opportunities to develop their ICT capabilities in all areas specified by the national curriculum.
- To allow pupils to gain confidence and enjoyment from their ICT activities and to develop skills which extend and enhance their learning throughout the curriculum.
- *To develop pupils' awareness of the use of computers not only in the classroom, but in everyday life.*
- To give children opportunities to personalise their own learning and assess themselves.
- To allow pupils to evaluate the potential of computers and also their limitations.
- To develop logical thinking and problem solving.
- To provide opportunities for pupils to gain knowledge about ICT tools. These include word-processors, databases, control devices, graphics and software for processing sound and images.
- To encourage pupils to become autonomous, independent users of ICT both as a learning resource and as a discipline in its own right.
- To develop a whole school approach to ICT ensuring continuity and progression.
- To explore their attitudes towards ICT and its value to them and society in general. For example, to learn about issues of security, confidentiality and accuracy and safety.

The aims of ICT within our school are to enable teachers and support staff:

- To use ICT to enable teachers to raise attainment levels.
- *To give teachers the tools they need to personalise our children's learning.*

- To use presentation software such as Smart Notebook and Powerpoint to provide interactive teaching resources.
- To use *the wealth of online learning resources to stimulate our children's interest in their learning and to provide for their different learning styles.*
- To build ICT into all areas of the curriculum so that children can have regular access to ICT as part of their core and creative curriculum.

Resourcing our ICT Provision

The strength of ICT within our school is that it can provide equality of access to the curriculum for all children - which allows them to function as their level and gives teachers the opportunity to personalise their learning wherever possible. ICT can act as an aid to communication or a means of controlling their environment, as well as an integrated aid to learning. The provision of resources should take into account the needs, abilities and interests of all children, especially:

- Children who have a special skill or talent.
- Children who speak a language other than English.
- Children from all backgrounds.
- Children who experience difficulties with learning.
- Children with physical and sensory difficulties.
- Children who have behavioural issues.
- Equality of opportunities for both girls and boys.

With this in mind, the Computing Team has focused on resourcing our school to deal with these priorities. We now have in place the following hardware and software:

- Smartboards in every classroom.
- At least 1 PC in every classroom.
- A fully functioning 30 PC ICT Suite equipped with headphones and microphones.
- Three 16 PC Laptop Trolleys.
- If needed, teaching staff have their own laptop for planning and creating teaching resources.
- A set of iPads for teaching staff
- A set of 16 Nintendo DS Lites with Brain Training.
- Three sets of 6 Beebots for teaching control in lower school.
- A set of 6 Probots for teaching control in upper school. These can be controlled from the school network using specific software.
- A Beebot set of floor maps and accessories for our SEN provision.
- A set of 6 data control logging boxes which monitor temperature, light and sound. These can download data from the control boxes direct to the school network using specific software.
- A set of heart monitoring equipment.
- A digital camera for each year group.
- A set of 6 Digiblue cameras for video and photography work.
- A set of 6 Digital cameras and tripods for animation / photography work.
- Subscription to Primary Espresso.
- Subscription to Education City.

- Subscription to Purple Mash
- Subscription to Mathletics.
- Subscription to Hamilton Trust,
- Subscription to Testbase.
- Subscription to SATS Tests Online
- Subscription to Bug Club.
- Penpals Software
- Descriptosaurus
- 30 Licenses for Clicker 5 for use in lower school and with EAL children.
- An Amazon Echo Dot

The Teaching of Computing

Although Computing skills are taught in timetabled Computing lessons - it is expected that it will not be taught in isolation. *Children's learning experiences* in Computing across the curriculum must support and reinforce each other. This requires that Computing skills are taught, not only in timetabled ICT lessons, but also in other areas of the curriculum. Our Computing provision should now be much more integrated into core and theme work.

Planning

During the academic year 2018-2019, teachers will be working with the New National Curriculum. The Computing Curriculum has vastly changed and teachers will be planning within the new curriculum as much as possible.

Assessment

This is subject to a review during the academic year, 2019/2020

Monitoring

During the academic year 2017/2018 monitoring of Long Term Planning was undertaken across school to ensure coverage of key curriculum areas in lessons and throughout the year. In September 2018, Long Term Planning was monitored again to check that planning meets the objectives covered in the national curriculum.

In 2018-2019 more detailed monitoring will be undertaken to ensure that LTP and MTP is translated into weekly plans and lessons.

Differentiation

Differentiation should be achieved both through differentiated activities and through differentiation of intended outcomes. For example pupils who are progressing rapidly should be encouraged to extend their Computing experiences.

Saving of Pupil Work on the Server

All pupils should save their work systematically on the server so that we can track developing pupil progress in Computing. At the beginning of every year, pupils should set up a new folder, to save their work, from that year. Year 1 & 2 teachers may wish to ask the Computing Team to help them to set up folders. Pupils in Years 3 ➤ 6 should set up their own folders in their own areas. Children can log onto computers using the unique login for each computer in school.

Roles and Responsibilities

The Role of the Senior Leadership Team

The Senior Leadership Team have overall responsibility for ICT. The Deputy Headteacher, in consultation with the Computing and teaching staff:

- Determines the way Computing should support, enrich and extend the curriculum.
- Decides the provision and allocation of resources.
- Ensures that Computing is used in a way to achieve the aims and objectives of the school.
- Ensures that there is a Computing policy and online safety policy.

The Role of the Computing Team

The Computing Team:

- Ensure a whole school approach to planning, teaching, assessment and record keeping for Computing.
- Ensure the implementation of the National Curriculum 2014 requirements for the Computing curriculum.
- Encourage colleagues and helps to develop computing skills to support teaching and learning.
- Promote and advise on the integration of Computing within appropriate teaching and learning activities across the whole curriculum.
- Co-ordinate the purchase of equipment.
- *Co-ordinates the evaluation and review of the school's* Computing policy.
- Highlights areas for development of Computing within the HAPI.

The Role of Subject Leaders

Subject leaders should, as part of their subject co-ordination:

- Develop and monitor cross-curricular use of Computing within their subject areas
- Suggest purchases of subject specific software.
- Develop budget bids which include purchase of software to enable delivery of their curriculum areas through Computing or recommend purchase using Computing allocation.
- Monitor the teaching and learning in their subject area, including ICT and online safety.

The Role of Teachers

Teachers play the greatest part in ensuring that the new Computing Curriculum is taught within our school and is delivered to its full potential. With this in mind, teachers:

- Are responsible for planning, teaching, assessment and record keeping for Computing for their year groups.
- Ensure that they are fully prepared and familiar with the content of each lesson they teach and the software applications needed to deliver their lessons.

- Assist the Computing co-ordinator and Team in the monitoring and recording of pupil progress in Computing.
- Implement the Internet Acceptable Use Policy and appropriate Internet Safety Education.
- Ensure that guidelines for health and safety of pupils and staff are adhered to.
- Are responsible for informing the ICT Manager of any technical problems with ICT equipment or work required by filling in a *“Help Desk” report, which is available on the Staff Portal.*

Staff Development

INSET will be provided as either school based training or through courses run by the LEA or other providers. If whole school INSET is not appropriate staff will be encouraged to attend relevant courses or use peer training as another method of staff development.

Continuity and Progression in Computing

Computing Curriculum planning should ensure continuity and progression. The school recognises that progression in Computing involves four main aspects:

- *The progressive development of pupils’ skills, knowledge and understanding*
- breadth of ICT applications
- Increased complexity in which Computing is applied
- The growing autonomy of the pupil in their learning.
- The ability of the learner to personalise their learning.

Pupils with Special Educational Needs

Pupils with Special Educational Needs have the same Computing entitlement as all other pupils and are offered the same curriculum. However, in addition particular applications of Computing are used for:

- Pupils with difficulties in learning, who need to be motivated to practice skills regularly and intensively, and thus benefit from the use of programmes in which skills practice is set in the context of a motivating game.
- Certain pupils with physical or communication difficulties may have their own specially adapted machines for use in communication and across the curriculum.
- Pupils of higher ability may be extended through the use of programmes which offer challenge and opportunities for investigation.

The Internet

The use of the Internet will continue to be embedded within the new curriculum. Our internet provision provides web-filtering software, which protects the pupils from undesirable materials. Since no technological solution can be 100 per cent effective in guaranteeing safety when using the Internet, we minimise the risks to pupils by implementing a clear Internet Acceptable Use Policy and appropriate Internet safety education.

New Equipment

We ensure that we constantly have a high number of computers in school in relation to the number of children by following a planned replacement programme for older computers. We budget to achieve this aim, to avoid 'spikes' of expenditure by suggesting an annual sum to be set aside to cover equipment replacement. New equipment will be purchased on a rolling programme.

Health and Safety

It is imperative that all electrical equipment is kept in good working order. To ensure the health and safety of pupils and staff the following guidelines must be adhered to:

- Pupils should not be allowed to switch on the power at the mains.
- Equipment and leads should be situated away from water.
- Pupils should always be supervised when using electrical equipment.
- All plugs, leads and equipment will be checked regularly and tested for electrical safety every year.
- Pupils are not allowed to carry heavy equipment at any time.
- All pupils and staff using computers must take regular breaks to avoid eyestrain.
- When pupils are using computers the position and height of the chair must be appropriate.
- Pupils and staff must avoid looking into the beam of projectors.
- All equipment that is no longer needed or is unable to be repaired will be disposed of correctly according to the LEA's guidelines.

Policy Update

The speed and nature of technological development is such that a major update should be undertaken at least every year and minor updates as necessary.

School online safety Policy

Writing and Reviewing the online safety Policy

The online safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

The school will appoint an online safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap. It is not a technical role.

Our online safety Policy has been written by the school, building on the Education Leeds Online safety Policy and government guidance. It has been agreed by senior management and approved by governors.

The online safety Policy was revised by: _____ Date: _____

It was approved by the Governors on: _____

The next review date is (at least annually): _____

Introduction

The school makes widespread use of modern technology in the belief and understanding that it can develop and enhance all aspects of teaching and learning, as well as providing a preparation for life in a society where the use of ICT is widespread.

The statutory curriculum expects pupils to learn how to locate, retrieve and exchange information using ICT.

This policy:

- applies to all users of ICT equipment, in its widest sense, whilst on school premises. It also applies to anyone who uses school ICT equipment, software or electronic data whilst off the premises.
- *forms part of the school's* Computing Policy and ICT Acceptable Use Policy.
- relates to other school policies including, child protection, behaviour and bullying.
- also relates to the Internet Access Policy & Email Code of Practice.
- often refers to the internet due to this being the major concern. However, it should be noted that there are other aspects of online safety that need consideration.

It is difficult to consider every eventuality within this policy due to the nature of rapid technological change within short timescales.

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

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, including those which could lead to radicalisation or extremism
- content validation: how to check authenticity and accuracy of online content

Contact:

- grooming
- cyber-bullying in all forms

- *identity theft (including 'frape' (hacking Facebook profiles) and sharing passwords*

Conduct:

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- 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 Ofsted Inspecting e-safety in schools April 2014)

Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2021
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- *Using the school's ICT facilities to breach intellectual property rights or copyright*
- *Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination*
- *Breaching the school's policies or procedures*

- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- *Connecting any device to the school's ICT network without approval from authorised personnel*
- *Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data*
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the *school's ICT facilities*
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using *websites or mechanisms to bypass the school's filtering mechanisms*
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use *of the school's ICT facilities*. Exceptions can be found in the Unacceptable Use section.

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the *headteacher's discretion*.

If such a situation arose, the headteacher would be approached and the situation would need to be sufficiently explained and considered before any permission was granted.

Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies in the staff code of conduct. Copies of this policy can be found on the New Staff Network or can be accessed by asking Sam Wiltshaw, the school Business Manager. Copies of this policy are available on Parago.

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Harehills Primary School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of Harehills Primary School.
- 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 cyberbullying 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.

Communication:

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

- Policy to be posted on the school website
- Policy to be part of school induction pack for all staff to read at the start of each new academic year/as part of induction for new staff into school.
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be held in classroom Investors in Pupils files and office files.

Online Safety

The increased use of technology at work and at home exposes people to a number of risks and dangers. In its simplest form online safety is about ensuring people use electronic technologies in a way which will keep them safe without limiting their opportunities for creation and innovation.

The Internet is fantastic for information and great for communication, but we all need to know how to use it safely. The children are likely to have internet access in more than one place, so it is important to equip them with the skills to handle this technology safely.

Online safety is also about protecting the hardware and software we use from attack by unscrupulous people, who may wish to cause disruption or commit illegal acts.

Online safety is also about protecting electronic data, our private, personal data and that of other people.

Responsibilities

The use of computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.

Everyone who uses ICT connected with the school has a responsibility to have a regard for online safety.

The Government has placed a responsibility on the Governors and Management of the school to ensure that all employees and pupils are aware of online safety concerns and procedures, and that they receive training to raise their awareness of the issues involved.

The teaching staff have a responsibility, as part of the statutory requirements of the curriculum, to teach online safety.

Although the ultimate responsibility lies with the Governing Body and the Head teacher, the school will nominate:

- an online safety lead(s) within the computing team.
- a Governor with responsibility for online safety issues.
- a member of the senior management team to deal with online safety issues and online safety complaints in particular.

The computing team will:

- oversee the development of this policy
- oversee the implementation of this policy
- advise the school management on online safety issues
- advise staff on online safety teaching and learning resources
- be a point of contact for anyone connected with the school who has questions or concerns about online safety issues
- be available to deal with general issues of online safety that are not specific complaints concerning individuals (for example: informing the ICT Manager of an inappropriate website or a security issue)
- be available to deal with minor infringements of the online safety policy and rules, including accidental infringements

- pass on to a nominated senior manager or Head Teacher any complaint or evidence received concerning individual pupils or staff misuse of ICT

Teaching and Learning

Why the Internet and digital communications are important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

The school Internet access is facilitated through EXA Networks for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Pupils will be shown how to publish and present information to a wider audience.

Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

The school has a progressive online safety education programme as part of the computing curriculum / PSHE curriculum. This will include online safety lessons being taught each half term. This covers a range of skills and behaviours appropriate to their age and experience, including:

- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy;
- to be aware that the author of a web site / 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 on-line *'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;
- *[for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;*
- that pupils will be taught the importance of cross-checking information before accepting its accuracy.
- that pupils are taught how to report unpleasant Internet content by telling a teacher. To know how to report any abuse including cyberbullying; pupils are taught 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 (Hectar). The teacher must report this to the ICT Manager or Safeguarding team.
- that Internet use is planned carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- that students will be reminded about their responsibilities through an Acceptable Use Agreement which every student will sign which be kept in the Investors in Pupils File located in every classroom
- ensuring staff will model safe and responsible behaviour in their own use of technology during lessons.
- ensuring 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;
- ensuring 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 on-line; on-line gaming / gambling;

Children with Special Needs

ICT can be a positive tool for children with Special Educational Needs. Access to the Internet is therefore a vital link with which communication to the outside world can be achieved. Access to the Internet can also stimulate children to develop their ideas and research independently.

The school will endeavour to ensure that children with Special Educational Needs are made aware of the risks and dangers of using ICT, within their understanding and abilities. The ICT Coordinator will make appropriate resources available to facilitate this.

Managing Internet Access

Access to school ICT facilities and materials

The school's IT Manager in conjunction with the Computing Team *manages access to the school's ICT facilities and materials* for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when *accessing the school's ICT facilities*.

Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email accounts.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as *paper documents*. *Deletion from a user's inbox* does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the School Business Manager, Sam Willtshaw, immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business. In some instances staff may use a phone that is not a work phone to make calls, so long as the caller ID has been masked. Wherever possible, work phones should be used.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in Unacceptable Use.

Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The School Business Manager, Sam Willshaw, and Head Teacher, Jo Summerfield, may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching hours
- Does not constitute 'unacceptable use', as defined in section Unacceptable Use
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's Personal Device Policy.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email to protect themselves online and avoid compromising their professional integrity.

Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

School Social Media Accounts

N/A

Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts

- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Pupils

Access to ICT facilities

- *Computers and equipment in the school's ICT suite are available* to pupils only under the supervision of staff
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Pupils will be provided with an email account linked to Pupil Mail which can only be used to send and receive e-mails within a closed network.

Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the Behaviour Policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- *Breaching the school's policies or procedures*
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community

- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the *school's ICT facilities*
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

Handling online safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Complaints of a child protection nature must be dealt with in accordance with school's Safeguarding Policy.
- Pupils and parents will be informed of the complaints procedure via the Harehills website under the family tab.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- Discussions will be held with the school police contact to establish procedures for handling potentially illegal issues.

Pupil Email

- Pupils may only use Pupil Mail in school to access and send e-mails.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Pupil email is limited to internal use only.
- The forwarding of chain letters is not permitted.

Parents

Access to ICT facilities and materials

Parents do not *have access to the school's ICT facilities as a matter of course*. However, parents working for, or with the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate *level of access, or be permitted to use the school's facilities at the headteacher's discretion*.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online. Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website.

Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot *guarantee security*. *Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.*

Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement *and maintain to protect personal data and the school's ICT facilities.*

Any personal devices using the school's *network must all be configured in this way.*

Data protection

All personal data must be processed and stored in line with data protection regulations *and the school's data protection policy.*

The School's *Data Protection Policy can be found on Parago*. A Hard Copy is available from the office.

Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert their line manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

Protection from cyber attacks

The school will:

Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure

Provide annual training for staff (and include this training in any induction for new starters, if they join *outside of the school's annual training window*) *on the basics of cyber security*, including how to:

- Check the sender address in an email
- Respond to a request for bank details, personal information or login details

- Verify requests for payments or changes to information

Make sure staff are aware of its procedures for reporting and responding to cyber security incidents

Investigate whether our IT software needs updating or replacing to be more secure

Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data

Put controls in place that are:

- **'Proportionate'**: the school will verify this using a third-party audit annually to objectively test that what it has in place is up to scratch
- **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
- **Up-to-date**: with a system in place to monitor when the school needs to update its software
- **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be

Back up critical data once a day and store these backups on [cloud based backup systems/external hard drives that aren't connected to the school network and which can be stored off the school premises]

Delegate specific responsibility for maintaining the security of our management information system (MIS) to Computer Manager

Make sure staff:

- Enable multi-factor authentication where they can, on things like school email accounts
- Store passwords securely using a password manager
- *All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.*
- Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.
- Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.
- All staff will use a password manager to help them store their passwords securely. Teachers will generate passwords for pupils using a password manager/generator and keep these in a secure location in case pupils lose or forget their passwords.

Make sure ICT staff:

- Conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department, for example, including how the school will communicate with everyone if communications go down, who

will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested once a year and after a significant event has occurred, *using the NCSC's 'Exercise in a Box'*

- Work with our Local Authority to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

This school:

- Has the educational filtered secure broadband connectivity through EXA Networks
- Uses EXA Networks filtering system which blocks sites that fall into categories such as:
 - Pornography
 - Race hatred, including those which could lead to radicalisation or extremism and that staff are aware of the dangers these sites pose
 - 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;*
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensures network healthy through use of Sophos anti-virus software etc. and network set-up so staff and pupils cannot download executable files;
- Uses approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites;
- Only unblocks other external social networking sites for investigative purposes;
- 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;
- Works in partnership with EXA Networks 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;*
- Ensures all staff and students have signed an Acceptable Use Agreement and understand that they must report any concerns;
- Requires staff to preview websites before use [where not previously viewed or cached] . 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 ICT Manager. Our ICT Manager logs or escalates as appropriate to the technical service provider (EXA Network) as necessary;
- *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;*
- 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.

Internet access

The school wireless internet connection is secured.

Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's visitor wifi (Harehills Guest) in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Published content and the school web site

Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.

The Head Teacher and Governors will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs. This is recommended by CEOPS as it stops people who do not know a child being able to identify them outside school.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

Pupil image file names will not refer to the pupil by name.

Parents should be clearly informed of the school policy on image taking and publishing

The school will block access to social networking sites. Although the school recognises that primary age children should not be on social media sites it will consider how to educate pupils in their safe use.

Newsgroups will be blocked unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Managing technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

The Senior Leadership Team should note that technologies such as mobile phones with Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Children are forbidden from bringing mobile phones to school.

Games machines including the Nintendo DSi and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location. This must be taken into consideration for further purchases of handheld games machines.

Policy Decisions

Authorising Internet access

All staff must read and sign the “Staff Code of Conduct for ICT” before using any school ICT resource.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line material.

In Key Stage 2, children will be given their own email account details. They are introduced to, and use e-mail as part of the ICT/Computing scheme of work.

Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;

Has set-up 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;

Parents will be asked to sign and return a form to consent the use of the Internet at the start of each new school year.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor EXA Networks can accept liability for any material accessed, or any consequences of Internet access.

The school should audit ICT use to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate and effective.

Community Access to the Internet

The school will not allow external out of school lettings to use the Internet from school unless this has been agreed with the Head teacher and the appropriate consent form signed.

The school will liaise with local organisations to establish a common approach to online safety.

Communications Policy

Introducing the online safety policy to pupils

Online safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.

Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

A programme of training in online safety will be developed, possibly based on the materials from CEOP.

Online safety training will be embedded within the Computing curriculum or the Personal Social and Health Education (PSHCE) curriculum.

Staff and the online safety policy

All staff will be given the School online safety Policy and its importance explained.

Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

Staff that manage filtering systems or monitor ICT use will be supervised by a member of senior management and work to clear procedures for reporting issues.

Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the School online safety Policy in newsletters, the school brochure and on the school Web site.

The school will maintain a list of online safety resources for parents/carers.

The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Staff Code of Conduct for ICT

To ensure that all members of staff are fully aware of their professional responsibilities when using information systems and when communicating with each other and pupils, you are asked to sign this **code of conduct**. **Members of staff should consult the school's online safety policy** for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Head teacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely in accordance to the GDPR privacy statement.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding *children's safety* to the Designated Child Protection Coordinator or Head teacher.
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted. (Do not add current *pupils as "friends"* and consider carefully about the ex-pupils still in FT education as "friends" on Facebook or other social networking sites.) I know I should not access these facilities during directed time or by using school equipment. During access to such sites either in or out of school, I will not comment on this school or any persons in it, which might bring the school into disrepute.
- I will promote online safety with students in my care at the start of each half term and in computing lessons and will help them to develop a responsible attitude to system use, communications and publishing.
- The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Print Name: _____ Sign: _____ Date: _____

HAREHILLS PRIMARY SCHOOL

Code of Conduct for the Acceptable Use of ICT

Year 1 and Year 2 Pupils

ICT means Information & Communication Technology and includes:

Computers, the school computer network, laptops, the school e-mail, the Internet, webcams, digital cameras, mobile phones, memory sticks, computer disks, games consoles (especially those that have internet connection or a built in camera), DVDs, CDs, DVD/video/CD players, mp3 players, I-pods and many other devices that can be operated by connecting them to a computer.

The school uses ICT to help me with my learning.

The school does its best to keep me safe when I am using ICT.

This is part of my learning about Online safety.



I understand that

- The school makes these rules so as to be fair to everyone.
- The school will keep a record of everything I do on the school computers.
- If I deliberately break these rules I will get into trouble.



I will

- Always ask permission from a member of staff before I use any ICT equipment in school.
- Use school ICT in a sensible and responsible way.
- Only use my own username and password when I log on to a school computer.
- Tell a member of staff straight away if I accidentally do something that I know I am not supposed to do with school ICT equipment.
- Tell a member of staff if I see anything on a school computer that upsets me or I do not like.



I will not

- Use a mobile phone at school.
- Deliberately use ICT to cause harm or be nasty to another person.



Full name

Class

Date for the school year ____ / ____

HAREHILLS PRIMARY SCHOOL

Code of Conduct for the Acceptable Use of ICT

Year 3, Year 4, Year 5 and Year 6 Pupils

The school uses ICT to help me with my learning.
The school does its best to keep me safe when I am using ICT.

This is part of my learning about online safety.

I understand that

- The school makes these rules to keep me, my family and my friends safe.
- The school makes these rules so as to be fair to everyone.
- The school will keep a record of everything I do on the school computers, the Internet sites I visit and all my e-mails.
- If I deliberately break these rules I will get into trouble,
- my parent / carer may be told and I may not be allowed to use school ICT equipment.



I will

- Always ask permission from a member of staff before I use any ICT equipment in school.
- Always ask permission from a teacher before I use the Internet or use e-mail.
- Use school ICT in a sensible and responsible way.
- Do my best to look after school ICT equipment properly.
- Only use my own username and password when I log on to a school computer.
- Keep my login and e-mail password secret.
- *Follow the school's "Rules for Responsible Internet Use"* when I am using the Internet (EXA Network).
- Save my work in my own user area on the school network.
- Ask permission before I save any work in the Resources drive of the school network.
- Tell a member of staff straight away if I accidentally do something that I know I am not supposed to do with school ICT equipment.



I will not



- Use school equipment without permission.
- Use a mobile phone on school premises.
- Take digital photographs, or use a webcam, on school premises without permission from the Head teacher.
- Use computer equipment from home whilst on school premises.
- Use any computer disk or memory stick from home on any school computer.
- Use any other ICT equipment from home, including any games machine or console that has a built in camera, webcam, internet access or wireless connection.
- *Use another person's username and password.*
- *Deliberately look at other people's computer files without permission.*
- Deliberately use ICT to cause harm or be nasty to another person.



I agree to obey this code of conduct for the school year ____/____

Signature

Class

Date

Full Name (printed)

Information & Communication Technology includes:

Computers, the school computer network, laptops, Fizz Books, the school network, e-mail, the Internet, webcams, digital cameras, mobile phones, memory sticks, computer disks, games consoles (especially those that have internet connection or a built in camera), DVDs, CDs, DVD/video/CD players, mp3 players, I-pods and many other devices that can be operated by connecting them to a computer.

Please see Appendix 1 for addition guidance on online safety guidance.