Holly Primary School

Computing

**Whole School Policy
& Documentation**

Spring 2026

Contents

Introduction

The use of computers and computer systems is an integral part of the National Curriculum and knowing how they work is a key life skill. In an increasingly digital world there now exists a wealth of software, tools and technologies that can be used to communicate, collaborate, express ideas and create digital content. At Holly Primary School we recognise that pupils are entitled to a broad and balanced computing education with a structured, progressive, approach to the learning how computer systems work, the use of IT and the skills necessary to become digitally literate and participate fully in the modern world. The purpose of this policy is to state how the school intends to make this provision.

Aims

The school's aims are to:

- Provide a broad, balanced, challenging and enjoyable curriculum for all pupils.
- Develop pupil's computational thinking skills that will benefit them throughout their lives.
- Meet the requirements of the national curriculum programmes of study for computing at Key Stage 1 and 2
- To respond to new developments in technology
- To equip pupils with the confidence and skills to use digital tools and technologies throughout their lives.
- To enhance and enrich learning in other areas of the curriculum using IT and computing.
- To develop the understanding of how to use computers and digital tools safely and responsibly.

The National Curriculum for Computing aims to ensure that all pupils:

- Can understand and apply the fundamental principles of computer science, including logic, algorithms, data representation, and communication.
- Can analyse problems in computational terms, and have repeated practical experience of writing computer programs in order to solve such problems.
- Can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems.
- Are responsible, competent, confident and creative users of information and communication technology.

Rationale

The school believes that I.T, computer science and digital literacy:

- Are essential life skills necessary to fully participate in the modern digital world.
- Allows children to become creators of digital content rather than simply consumers of it.
- Provides access to a rich and varied source of information and content.
- Communicates and presents information in new ways, which helps pupils understand, access and use it more readily.
- Can motivate and enthuse pupils.
- Offers opportunities for communication and collaboration through group working both inside and outside of school.
- Has the flexibility to meet the individual needs and abilities of each pupil.

Curriculum Objectives

By the end of key stage 1 pupils should be taught to:

- Understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following a sequence of instructions.
- Write and test simple programs.
- Use logical reasoning to predict and computing the behaviour of simple programs.
- Organise, store, manipulate and retrieve data in a range of digital formats.
- Communicate safely and respectfully online, keeping personal information private, and recognise common uses of information technology beyond school.

By the end of key stage 2 pupils should be taught to:

- Design and write programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts.
- Use sequence, selection, and repetition in programs; work with variables and various forms of input and output; generate appropriate inputs and predicted outputs to test programs.
- Use logical reasoning to explain how a simple algorithm works and to detect and correct errors in algorithms and programs.
- Understand computer networks including the internet; how they can provide multiple services, such as the world-wide web; and the opportunities they offer for communication and collaboration.
- Describe how internet search engines find and store data; use search engines effectively; be discerning in evaluating digital content; respect individuals and intellectual property; use technology responsibly, securely and safely.
- Select, use and combine a variety of software (including internet services) on a range of digital devices to accomplish given goals, including collecting, analysing, evaluating and presenting data and information.

Resources and Access

The school acknowledges the need to continually maintain, update and develop its resources and to make progress towards consistent, compatible computer systems by investing in resources that will effectively deliver the objectives of the National Curriculum and support the use of IT, computer science and digital literacy across the school. Teachers are required to inform the computing subject leader of any faults as soon as they are noticed. Resources if not classroom based are located in the computing suite. A service level agreement with ATOMIT is currently in place to help support the subject leader to fulfill this role both in hardware & software. Computing network infrastructure and equipment has been sited so that:

- Every classroom from nursery to Y6 has an interactive monitor with sound, and video streaming facilities.
- 30 Winbooks are shared between Y5/6
- 30 Winbooks are shared between Y3/4
- 30 Chromebooks aer shared between Y1/2
- Internet access is available in all classrooms.
- The laptops and iPads are available for use throughout the school day as part of computing lessons and for cross-curricular use.
- Pupils may use IT and computing independently, in pairs, alongside a TA, or in a group with a teacher.
- The school has a computing technician who is in school monthly.
- A governor will be invited to take a particular interest in computing in the school.

Artificial Intelligence (AI)

Artificial Intelligence (AI) is increasingly present in education and wider society. In school settings, AI can support learning, inclusion, and staff efficiency when used appropriately. However, it also presents potential risks relating to safeguarding, data protection, accuracy, and over-reliance. This section sets out how AI will be used safely, responsibly, and transparently within our school.

Aims
• Ensure AI use supports high-quality teaching and learning
• Safeguard pupils' wellbeing, privacy, and data at all times
• Develop pupils' understanding of AI in an age-appropriate way
• Maintain clear human oversight and professional judgement

Our Approach
The school adopts a proactive but cautious approach to AI. AI will only be used where it provides a clear educational or operational benefit and where risks have been carefully considered. AI will support, not replace, professional practice or pupils' own thinking and creativity. AI use in school will be safe, purposeful, transparent, and inclusive.

Use of AI by Pupils
Pupils may only use AI tools that are approved by the school and under direct teacher supervision. Pupils are taught that AI is a tool created by people, that it can make mistakes, and that its outputs should be questioned and checked. Pupils must not enter personal information, use AI to complete work on their behalf, access unapproved tools, or create inappropriate content.

Use of AI by Staff
Staff may use AI to support professional tasks such as planning, resource creation, differentiation, or drafting communications. Staff must review and verify all AI-generated content, retain responsibility for decisions, and follow all data protection requirements.

Safeguarding, Data Protection, and Accuracy
Only AI tools that meet safeguarding, age-appropriateness, and data protection requirements will be approved. All AI use aligns with the school's safeguarding, online safety, and data protection policies. Teachers remain responsible for checking accuracy, suitability, and potential bias.

Monitoring and Review
AI use is overseen by senior leaders and reviewed regularly to ensure it remains safe, effective, and compliant with statutory guidance.

Planning

The school uses the Holly Computing Curriculum - the whole-school scheme of work. It fully meets the objectives of the National Curriculum for Computing and allows for clear progression in computing.

A minority of children will have particular teaching and learning requirements which go beyond the provision for that age range and if not addressed, could create barriers to learning. This could include G&T children, those with SEN or those who have EAL. Teachers must take account of these requirements and plan, where necessary, to support individuals or groups of pupils to enable them to participate effectively in the curriculum and assessment activities. During any teaching activities, teachers should bear in mind that special arrangements could be made available to support individual pupils. This is in accordance with the school inclusion policy. These children should be identified and discussed at pupil progress meetings to ensure that appropriate provisions and/or interventions are affected.

Assessment and Record Keeping

Teachers regularly assess progress through observations and evidence. Key objectives to be assessed are taken from the National Curriculum to assess computing each term. Assessing computing is an integral part of teaching & learning and key to good practice.

Assessment is process orientated - reviewing the way that techniques and skills are applied purposefully by pupils to demonstrate their understanding of computing concepts. As assessment is part of the learning process, it is essential that pupils are closely involved. Assessment can be broken down into;

- Formative assessments are carried out during and following short focused tasks and activities. They provide pupils and teaching staff the opportunity to reflect on their learning in the context of the agreed success criteria. This feeds into planning for the next lesson or activity.
- Summative assessment should review pupils' ability and provide a best fit 'level'. Independent tasks provide a number of opportunities and scope for pupils to demonstrate their capability throughout the term. There should be an opportunity for pupil review and identification of next steps
- We assess the children's work in computing by making informal judgments as we observe the children during lessons. Once the children complete a unit of work, we make a summary judgment of the work for each pupil as to whether they have yet to obtain, have obtained or have exceeded the expectations of the unit and the children complete self-assessment.

The children's work is either saved in the cloud, within the website accounts being used, or printed and saved in their workbooks. Other cross-curricular work may be printed and filed within the subject from which the task was set.

Monitoring and Evaluation

The subject leader is responsible for monitoring the standard of the children's work and the quality of teaching in line with the schools monitoring cycle. This may be through lesson observations, pupil discussion and evaluating pupil work.

We allocate time for the vital task of reviewing samples of children's work and for visiting classes to observe teaching in the subject.

Pupils with Special Educational Needs (see also SEN policy)

We believe that all children have the right to access IT and computing. In order to ensure that children with special educational needs achieve to the best of their ability, it may be necessary to adapt the delivery of the computing curriculum for some pupils.

We teach IT and computing to all children, whatever their ability. Computing forms part of the national curriculum to provide a broad and balanced education for all children. Through the teaching of computing we provide opportunities that enable all pupils to make progress. We do this by setting suitable challenges and responding to each child's individual needs. Where appropriate IT can be used to support SEN children on a one to one basis where children receive additional support.

Equal Opportunities (see also equal opportunities policy)

We will ensure that all children are provided with the same learning opportunities regardless of social class, gender, culture, race, disability or learning difficulties. As a result, we hope to enable all children to develop positive attitudes towards others. All pupils have equal access to computing and all staff members follow the equal opportunities policy. Resources for SEN children and gifted & talented will be made available to support and challenge appropriately.

The Role of the Subject Leader

There is a computing subject leader who is responsible for the implementation of computing policy across the school. Their role is to:

- Offer help and support to all members of staff (including teaching assistants) in their teaching, planning and assessment of computing.
- Provide colleagues opportunities to observe good practice in the teaching of computing.
- Maintain resources and advise staff on the use of digital tools, technologies and resources.
- Monitor classroom teaching or planning following the schools monitoring program.
- Monitor the children's progression in computing, looking at examples of work of different abilities.
- Manage the computing budget.
- Keep up-to-date with new technological developments and communicate information and developments with colleagues.
- Lead staff training on new initiatives.
- Attend appropriate in-service training
- Have enthusiasm for computing and encourage staff to share this enthusiasm.
- Keep parents and governors informed on the implementation of computing in the school.
- Liaise with all members of staff on how to reach and improve on agreed targets
- Help staff to use assessment to inform future planning.

The Role of the Class Teacher

Individual teachers will be responsible for ensuring that pupils in their classes have opportunities for learning computing and using their knowledge, skills and understanding of computing across the curriculum.

They will plan and deliver the requirements of the National Curriculum for Computing to the best of their ability. We set high expectations for our pupils and provide opportunities for all to achieve, including girls and boys, pupils with educational special needs, pupils with disabilities pupils from all social and cultural backgrounds, and those from diverse linguistic backgrounds.

The class teacher's role is a vital role in the development of computing throughout the school and will ensure continued progression in learning and understanding, and create effective learning environments.

The class teacher will also:

- Secure pupil motivation and engagement.
- Provide equality of opportunity using a range of teaching approaches and techniques.
- Use appropriate assessment techniques and approaches.
- Set suitable targets for learning as outlined in the inclusion policy.

Staff Training

The computing subject leader will assess and address staff training needs as part of the annual development plan process or in response to individual needs and requests throughout the year.

Individual teachers should attempt to continually develop their own skills and knowledge, identify their own needs and notify the subject leader.

Teachers will be encouraged to use IT and computing to produce plans, reports, communications and teaching resources.

Health and Safety

The school is aware of the health and safety issues involved in children's use of IT and computing.

All fixed electrical appliances in school are tested by a Local Authority contractor every five years and all portable electrical equipment in school is tested by an external contractor every twelve months.

It is advised that staff should not bring their own electrical equipment in to school but, if this is necessary, equipment must be PAT tested before being used in school. This also applies to any equipment brought in to school by, for example, visitors running workshops, activities, etc. and it is the responsibility of the member of staff organising the workshop, etc. to advise those people.

All staff should visually check electrical equipment before they use it and take any damaged equipment out of use. Damaged equipment should then be reported to a computer technician, bursar or head teacher who will arrange for repair or disposal.

In addition:

- Children should not put plugs into sockets, or switch the sockets on.
- Trailing leads should be made safe behind the equipment.
- Liquids must not be taken near the electronic devices.
- Magnets must be kept away from all equipment.
- E-safety guidelines will be set out in the e-safety policy & Acceptable Use Policy.

Security

We take security very seriously. As such:

- The computing technician will be responsible for regularly updating anti-virus software.
- Use of IT and computing will be in line with the school's 'acceptable use policy'. All staff, volunteers and children must sign a copy of the schools AUP.
- Parents will be made aware of the 'acceptable use policy' at school entry and ks2.
- All pupils and parents will be aware of the school rules for responsible use of IT and computing and the internet and will understand the consequence of any misuse.

Monitoring and Filtering

The network device we use is a Fortinet firewall device, accepted by many networking professionals as the market-leading product. It is used in thousands of schools and libraries around the world, and comes with the following features:

- Automated updates keep defences up-to-date with the latest web site ratings.
- Granular blocking & filtering provides policy-based access control based on categories, websites, and individual pages.
- URL database with more than 75 categories and more than 47 million rated websites.
- Push and pull update options provide the fastest possible update times.
- Extensive coverage helps attain CIPA (US HR4577) and BECTA (UK) compliance as well as full compliance with the KCSIE guidelines.
- History of sites visited and blocked are logged.

Office 365 tool Power Bi will be used, a visual dashboard reporting tool.
Data dashboards give access to review and report on all Internet usage against any of the categories related to the new KCSIE guidance. Data is collected on an individual user basis due to the integration of our Internet management service with your school Active Directory. This method means that any school user who triggers a website block can be identified by user account as well as IP address and timestamp. All sites visited that breach the blocked categories are also listed. The integration with Active Directory also means we can provide differentiated user level access for staff and pupils at the point of login to your network.
Monitoring systems also report via email when a category breach is reported. All email alerts can be sent to any number of email addresses provided by your school and provide a real-time alert showing user, IP address, category breached, URL attempted and a timestamp of the attempt.

Cross Curricular Links

As a staff we are all aware that IT and computing skills should be developed through core and foundation subjects. Where appropriate, IT and computing should be incorporated into schemes of work for all subjects. IT and computing should be used to support learning in other subjects as well as developing computing knowledge, skills and understanding. Our school provides pupils with opportunities to enrich and deepen learning using cross-curricular approaches.
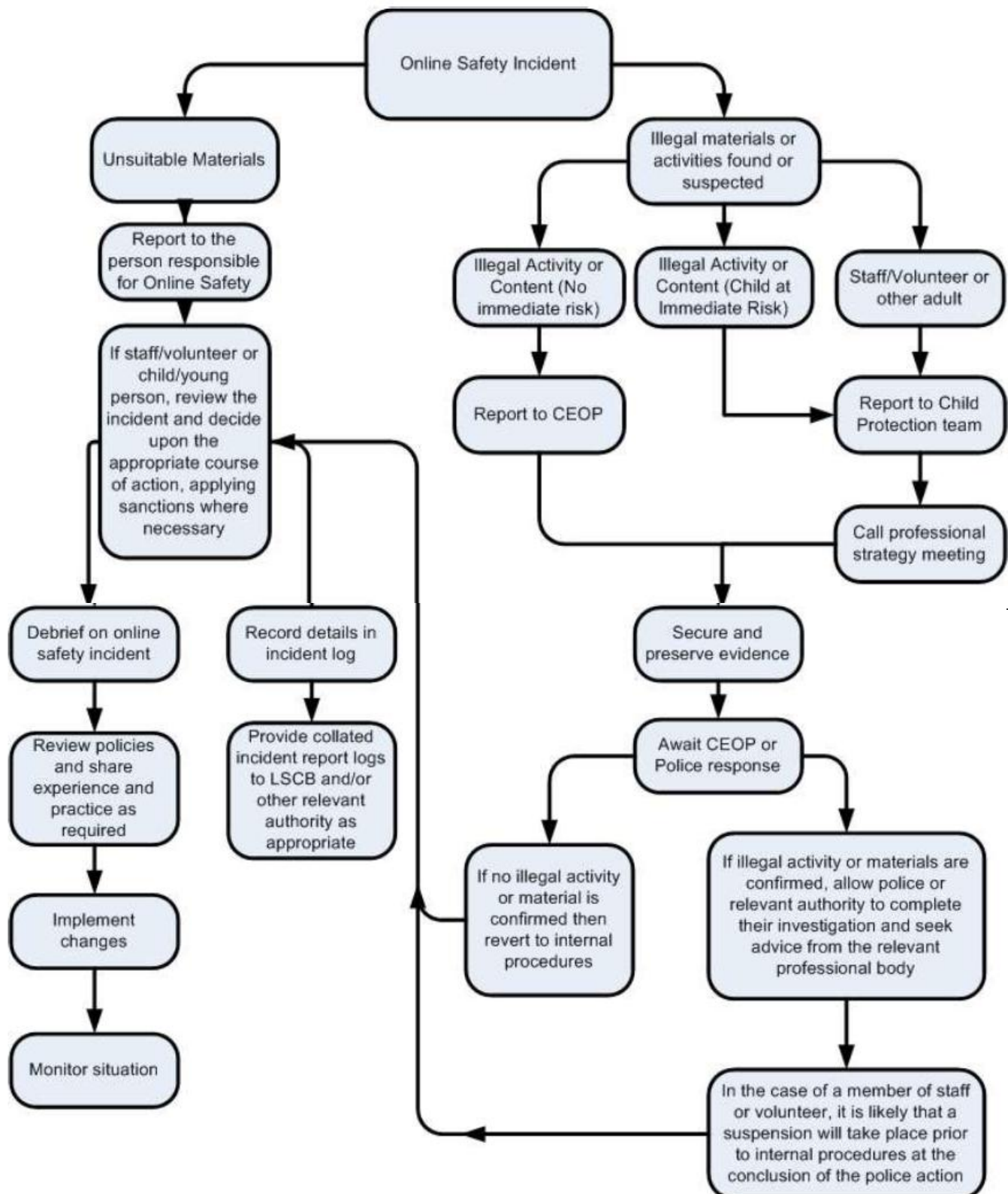
Parental Involvement

Parents are encouraged to support the implementation of IT and computing where possible by encouraging use of IT and computing skills at home for pleasure, through home-learning tasks and use of the school website. Parents will be made aware of issues surrounding e-safety and encouraged to promote this at home.

Incident Reporting

All stakeholders, and especially children, are actively encouraged to report incidents to the Headteacher, safeguarding lead and computing coordinator whether they occur in school or an external environment. The Headteacher, safeguarding lead and computing coordinator will log complaints, discuss an appropriate course of action and initiate it as soon as possible. Children are aware of procedures within school for reporting such incidents, however small, and school will deal with any concerns in a positive manner.

Illegal Incidents

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

```
                        ┌──────────────────────┐
                        │ Online Safety Incident│
                        └──────────────────────┘

┌──────────────────┐                    ┌──────────────────────┐
│ Unsuitable       │                    │ Illegal materials or │
│ Materials        │                    │ activities found or  │
└──────────────────┘                    │ suspected            │
                                        └──────────────────────┘

┌──────────────────┐       ┌──────────────┐ ┌──────────────┐ ┌──────────────┐
│ Report to the    │       │ Illegal      │ │ Illegal      │ │ Staff/       │
│ person responsible│      │ Activity or  │ │ Activity or  │ │ Volunteer or │
│ for Online Safety│       │ Content (No  │ │ Content (Child│ │ other adult  │
└──────────────────┘       │ immediate    │ │ at Immediate │ └──────────────┘
                           │ risk)        │ │ Risk)        │
┌──────────────────┐       └──────────────┘ └──────────────┘
│ If staff/volunteer│                                        ┌──────────────┐
│ or child/young   │       ┌──────────────┐                  │ Report to Child│
│ person, review the│      │ Report to CEOP│─────────────────▶│ Protection team│
│ incident and decide│     └──────────────┘                  └──────────────┘
│ upon the          │
│ appropriate course│                                        ┌──────────────┐
│ of action, applying│                                       │ Call professional│
│ sanctions where   │                                        │ strategy meeting│
│ necessary         │                                        └──────────────┘
└──────────────────┘

┌──────────────┐  ┌──────────────┐          ┌──────────────┐
│ Debrief on   │  │ Record details│          │ Secure and   │
│ online safety│  │ in incident   │          │ preserve     │
│ incident     │  │ log           │          │ evidence     │
└──────────────┘  └──────────────┘          └──────────────┘

┌──────────────┐  ┌──────────────┐          ┌──────────────┐
│ Review policies│ │ Provide collated│       │ Await CEOP or│
│ and share     │  │ incident report│        │ Police response│
│ experience and│  │ logs to LSCB  │         └──────────────┘
│ practice as   │  │ and/or other  │
│ required      │  │ relevant      │    ┌──────────────┐ ┌──────────────────┐
└──────────────┘  │ authority as  │    │ If no illegal│ │ If illegal activity│
                  │ appropriate   │    │ activity or  │ │ or materials are  │
┌──────────────┐  └──────────────┘    │ material is  │ │ confirmed, allow  │
│ Implement    │                       │ confirmed then│ │ police or relevant│
│ changes      │                       │ revert to    │ │ authority to      │
└──────────────┘                       │ internal     │ │ complete their    │
                                       │ procedures   │ │ investigation and │
┌──────────────┐                       └──────────────┘ │ seek advice from  │
│ Monitor      │                                        │ the relevant      │
│ situation    │                                        │ professional body │
└──────────────┘                                        └──────────────────┘

                                                        ┌──────────────────┐
                                                        │ In the case of a │
                                                        │ member of staff  │
                                                        │ or volunteer, it │
                                                        │ is likely that a │
                                                        │ suspension will  │
                                                        │ take place prior │
                                                        │ to internal      │
                                                        │ procedures at the│
                                                        │ conclusion of the│
                                                        │ police action    │
                                                        └──────────────────┘
```

How to respond if a risk is discovered

The E-safety lead will check that an adult follows these procedures in the event of any misuse of the Internet:

An inappropriate website is accessed inadvertently (ADULT): ·

- Report website to the E-Safety lead.
- Contact the IT Technician so that the site can be added to the banned or restricted list.
- Log the incident.

An inappropriate website is accessed inadvertently by a child or young person:

- Reassure the child/ young person
- Report website to the E-Safety lead.
- Contact the IT Technician so that the site can be added to the banned or restricted list.
- Log the incident.

An inappropriate website is accessed deliberately (Adult):

- Ensure that no one else can access the material by shutting down the computer.
- Log the incident.
- Report to the Principal and E-Safety lead immediately.
- Principal to refer back to the Acceptable Use Policy and follow agreed actions for discipline (see discipline policy).
- Inform the IT Technician in order to reassess the filters. An inappropriate website is accessed deliberately by a child or young person:
- Ensure that no one else can access the material by shutting down the computer.
- Log the incident.
- Inform E-Safety Lead
- Refer the child to the Acceptable Use Policy.
- Reinforce the knowledge that it is illegal to access certain images and police can be informed.
- Decide on appropriate sanction.
- Notify the parent/career.
- Contact the IT Technician to notify them of the website. 16 An adult receives inappropriate material:
- Do not forward this material to anyone else – doing so could be an illegal activity.
- Ensure the device is removed and log the nature of the material.

- Contact relevant authorities for further advice e.g. police, social care, LADO, CEOP.
- Log the incident

An illegal website is accessed or illegal material is found on a computer. (The following incidents must be reported directly to the police):

- Indecent images of children found. (Images of children whether they are or cartoons of children or young people apparently under the age of 16, involved in sexual activity or posed in a sexually provocative manner)
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.
- Criminally racist or anti-religious material
- Violent or bomb-making material
- Software piracy
- The promotion of illegal drug-taking
- Adult material that potentially breaches the obscene publications act in the UK.

If any of these are found, the following should occur:

- Alert the Headteacher and Safeguarding team lead immediately.
- DO NOT LOG OFF the computer but disconnect from the electricity supply.
- Contact the police and or CEOP and social care immediately (Police - 0161 856 8962, social care -0161 770 3790, children over 16 - 0161 770 6599, out of hours – 0161 770 6936). If a member of staff or volunteer is involved, refer to the allegations against staff in the Safeguarding Policy and report to the Local Authority Designated Officer.

An adult has communicated with a child or used ICT equipment inappropriately (e-mail/ text message etc.)

- Ensure the child is reassured and remove them from the situation.
- Report to the Headteacher and Designated Person for Child Protection immediately, who will then follow the Allegations Procedure and Child Protection Procedures as set out in the Safeguarding Policy
- Report to the Local Authority Designated Officer.
- Preserve the information received by the child if possible.
- Contact the police as necessary.

Threatening or malicious comments are posted to the school website or Office 365 TEAMS (or printed out) about an adult in school:

- Preserve any evidence and log the incident.
- Inform the Headteacher immediately and follow the Safeguarding Policy.

- Inform the E-Safety Lead so that new risks can be identified.
- Contact the police. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the Headteacher.

Threatening or malicious comments are posted to the school website or Office 365 TEAMS about a child in school or malicious text messages are sent to another child/young person (cyber bullying).

- Preserve any evidence
- Log the incident.
- Inform the E-Safety Lead and Principal.
- Contact parents/ careers.
- Refer to the Anti-Bullying Policy.
- Contact the police or CEOP as necessary

Legal Framework

This section is designed to inform users of legal issues relevant to the use of Communications. It is not professional advice.

The Sexual Offences Act 2003, The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an Offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images, such as videos, photos or web cams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with who they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape. More information about the 2003 Act can be found at www.teachernet.gov.uk

Communications Act 2003 (section 127) Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent; there is no need to prove any intent or purpose.

Data Protection Act 1998 The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 – 3) Regardless of an individual's motivation, the Act makes it a criminal offence to: gain access to computer files or software without permission (for example using someone else's password to access files); gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or impair the operation

Scope for Online Safety & Responsibilities

The following table of responsibilities applies to all members of Holly Primary School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to, and are users of, school computing systems, both in and out of Holly Primary School.

The Education and Inspections Act 2006 empowers Head teachers 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 Online bullying, or other Online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for, and of, electronic devices and the deletion of data (see appendix for template policy). 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 Online safety behaviour that take place out of school.

Key Responsibilities - **HEADTEACHER**
• To take overall responsibility for Online Safety provision.
• To take overall responsibility for data and data security (SIRO)
• 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 Online 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 ensure that there is a system in place to monitor and support staff who carry out internal Online safety procedures (e.g. network manager).

Key Responsibilities - **Online Safety Coordinator / Designated Child Protection Lead**

- Takes day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the school Online safety policies / documents
- Promotes an awareness and commitment to Online safeguarding throughout the school community
- Ensures that Online safety education is embedded across the curriculum
- Liaises with school computing technical staff
- To communicate regularly with SLT and the designated Online safety Governor / committee 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 Online Safety incident
- To ensure that an Online 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 on-line contact with adults / strangers
  - potential or actual incidents of grooming
  - online bullying and use of social media

Key Responsibilities - **Governors**

- To ensure that the school follows all current Online safety advice to keep the children and staff safe
- To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.
- To support the school in encouraging parents and the wider community to become engaged in e-safety activities
- The role of the Governors will include:
  - regular review with the Online Safety Co-ordinator / Officer (including
   Online safety incident logs, filtering / change control logs)

Key Responsibilities - **Computing Curriculum Leader**

- To oversee the delivery of the online safety element of the Computing curriculum
- To liaise with the online safety coordinator regularly
- To ensure that all data held on pupils on the OFFICE 365 TEAMS is adequately protected

Key Responsibilities - **Network Manager/technician/ATOM IT**

- To report any online safety related issues that arise, to the Online safety coordinator.
- 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 IT 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
- LGfL is informed of issues relating to the filtering applied by the Grid
- That he / she keeps up to date with the school's Online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the *network / Virtual Learning Environment (OFFICE 365 TEAMS) / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Online Safety Co-ordinator / Officer /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 online security and technical procedures

Key Responsibilities – **Data / Office Manager**

- To ensure that all data held on pupils on the school office machines have appropriate access controls in place
- To ensure that this information is in line with our GDPR policy

Key Responsibilities - **Teachers**

- To embed online 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

Key Responsibilities – **All Staff**

- To read, understand and help promote the school's e-safety policies and guidance
- To read, understand, sign and adhere to the school staff Acceptable Use Agreement
- To be aware of online safety issues related to the use of mobile phones, cameras and hand-held 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 online safety coordinator
- To maintain an awareness of current online safety issues and guidance e.g. through CPD
- To model safe, responsible and professional behaviour 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.

Key Responsibilities – **Pupils**

- Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy
- 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 hand-held devices.
- To know and understand school policy on the taking / use of images and on cyber-bullying.
- To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online 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

• Key Responsibilities – **Parents / Carers & External Groups**

- To support the school in promoting online safety and endorse 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 / OFFICE 365 TEAMS 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
- Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

Staff, Governor and Visitor
Digital Acceptable Use Agreement / Code of Conduct

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

- I will only use the school's email / Internet / Intranet / Office 365 and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, Office365 Outlook account for any school business.
- I will ensure that personal data is kept securely and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install software without permission of Colin Howard.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy, GDPR regulations, and with written consent of the parent, carer or staff member.
- Images will not be distributed outside the school network without the consent of the parent.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will not use my personal devices to record/photograph children during normal school based activities.
- I will support and promote the school's Online-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- As a member of staff, I understand this document forms part of the terms and conditions set out in my contract of employment.

Pupil (KS1) – Digital Acceptable Use Agreement

Holly
Primary School
Computing

o I will be POLITE Online.

o I will always ASK before taking a photograph or video of someone.

o I will keep my personal information PRIVATE.

o I will take good CARE of our equipment.

o I will not walk about the classroom with an open laptop.

o I will ASK an adult if I don't know what to do or think I have done something wrong.

o If something makes me WORRIED, I will TELL a trusted adult.

Date: September 2025

Name: _____

Pupil (KS2) - Digital Acceptable Use Agreement

Holly Primary School Computing

- 💻 I will be responsible for my good behaviour online, including public and private social media platforms and other messaging platforms such as Teams Messages or game chatrooms.

- 💻 I will always ask before taking a photograph or video of someone.

- 💻 I will not tell other people my passwords - I can tell my teacher, parent or trusted adult.

- 💻 I will not give out my personal details, such as my name, phone number and home address.

- 💻 I will be responsible for checking and setting my privacy settings on platforms I use.

- 💻 I will not deliberately search for, save, send, upload or attach anything that another person might think is unpleasant or nasty.

- 💻 If I am concerned or upset about anything I see, or something that is happening to me online including messages that I receive, I know I can talk to any adult in school, and my trusted adult at home.

- 💻 My school profile picture will not be a photo of me.

- 💻 If I need to bring a mobile phone to school, it will be kept turned off and in my teacher's desk. I will not use it until I have left the school grounds. – If I need to contact my parent before I leave school, I will stay with my teacher or go to the school office.

- 💻 I can help other pupils with their computing, but I won't touch their device.

- 💻 I know I can always bring in my device to school if I need to show something to an adult.

- 💻 It's not responsible to use Apps, Games or Websites that have an age restriction higher than my age – If I do use these, I will ask my parent if it's OK, and they can help me monitor my use.

- 💻 I know that my computing activity at school is monitored, and that my guardian contacted if an adult at school is concerned about my online safety or behaviour.

Date: September 2025
Name: _____

Viva Engage - Terms and Conditions

1. Posts and Comments
1. All adults will uphold and promote the values of our school and communicate in a positive, accurate, respectful and responsible manner.
2. All parents and carers are welcome to post their thoughts and ideas in the relevant pages, and to like, share and comment on postings. We request that you do this in a positive, respectful, constructive and accurate manner.
3. Public posts and private messages may only be sent between 8am and 6pm Monday to Friday, unless staff have children in their care during off-site visits and residential trips.
4. If followers have any specific concerns, particularly related to their own or other child/children, do not post these. Please speak directly to the child's class teacher or another member of staff as you would normally.
5. Under no circumstances should any child be named, described or discussed in public or private messages. We all have a responsibility to keep our children safe.

2. Posting documents, images and videos
1. Only school authorised administrators have permission to allow the upload of documents, photographs and videos.
2. Member's profile pictures can be personalised, but must not contain images of children.

3. Site moderation
1. The site will be monitored regularly by administrators that are authorised by the Head teacher.
2. All visitors to the pages are asked to inform Mr Howard/Mr White of any inappropriate comments, behaviours or concerns they have relating to the page so appropriate action can be taken as soon as possible.

4. Misuse
1. A post can be deleted by a member of staff without notification if they deem it to be inappropriate or breach any of these terms and conditions.
2. The head teacher can close any person's Viva Engage account and report directly to relevant external bodies if required.

5. Restrictions
1. The page is designed as a communication tool to engage with parents and carers. It is therefore restricted to people over 18 years of age.
2. Where the parent is under 18 years old, permission will be granted at the discretion of the head teacher.

6. Staff Responsibilities
1. Should a post require a response, Holly staff will do their best to reply within two school working days between the hours of 7.00am and 7.00pm.
2. It will be at the personal discretion of the staff if they reply to any comment on the site.
3. The private messaging facility exists but staff are under no obligation to check or respond to private messages. We would much rather speak to you in person.
4. Staff can reply to any comment on the Viva Engage feeds and will ensure that the information is correct before posting.

5. As we work in teams at Holly, we will try to post something at least once a week on the foundation page and each mixed year group site.
6. If a member of staff feels that any post does not uphold the positive ethos of Holly, or that it places them in a negative position by either naming them or through implication, they can request an administrator to take immediate action and delete the post without notifying the sender.
7. Staff will only post comments between 8am and 6pm Monday – Friday.

Website Policy

The School operates the following policy on its website regarding the use of photographs to ensure the privacy and safety of pupils at the school:

- Where pupils are named, only their first names are given;
- Where a pupil is named, no photograph of that pupil is displayed;
- Where a photograph is used which shows a pupil, no name is displayed.

By observing these points, the school ensures that visitors to the website cannot link images of pupils to names of pupils. The school follows a policy of seeking parents' permission before using images which show pupils on the website. No other private information about pupils is ever published on the website such as surnames or contact details.

Website Privacy Policy

We are committed to safeguarding the privacy of our website visitors; this policy sets out how we will treat your personal information.

- What information do we collect?
- We may collect, store and use the following kinds of personal data:
- Information about your visits to and use of this website;
- Information about any transactions carried out between you and us on or in relation to this website;
- Information that you provide to us for the purpose of registering with us, and/or leaving guestbook comments, and/or subscribing to our website services and/or email notifications. Information about website visits
- We may collect information about your computer and your visits to this website such as your IP address, geographical location, browser type, referral source, length of visit and number of page views. We may use this information in the administration of this website, to improve the website's usability, and for marketing purposes.
- We use cookies on this website. A cookie is a text file sent by a web server to a web

browser, and stored by the browser. The text file is then sent back to the server each time the browser requests a page from the server. This enables the web server to identify and track the web browser.

- We may send a cookie which may be stored by your browser on your computer's hard drive. We may use the information we obtain from the cookie in the administration of this website, to improve the website's usability and for marketing purposes. We may also use that information to recognise your computer when you visit our website, and to personalise our website for you.

- Most browsers allow you to refuse cookies. (For example, in Internet Explorer you can refuse all cookies by clicking "Tools", "Internet Options", "Privacy", and selecting "Block all cookies" using the sliding selector.) This will, however, have a negative impact upon the usability of many websites. Using your personal data Personal data submitted to this website will be used for the purposes specified in this privacy policy or in relevant parts of the website.

In addition to the uses identified elsewhere in this privacy policy, we may use your personal information to:

- Improve your browsing experience by personalising the website;
- Provide other organisations with statistical information about our users - but this information will not be used to identify any individual user. We will not without your express consent provide your personal information to any third parties for the purpose of direct marketing. Other disclosures
- In addition to the disclosures reasonably necessary for the purposes identified elsewhere in this privacy policy, we may disclose information about you:
- To the extent that we are required to do so by law;
- In connection with any legal proceedings or prospective legal proceedings;
- In order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk);
- Except as provided in this privacy policy, we will not provide your information to third parties. Security of your personal data We will take reasonable precautions to prevent the loss, misuse or alteration of your personal information. Of course, data transmission over the internet is inherently insecure, and we cannot guarantee the security of data sent over the internet. Policy amendments We may update this privacy policy from time-to-time by posting a new version on our website. You should check this page occasionally to ensure you are happy with any changes. Third party websites the website contains links to other websites. We are not responsible for the privacy policies of third-party websites. Website Disclaimer Introduction This disclaimer governs your use of our website; by using our website, you accept this disclaimer in full. If you disagree with any part of this disclaimer, do not use our website. Intellectual property rights Unless otherwise stated, we or our licensors own the intellectual property rights in the website and material on the website. Subject to the license below, all our intellectual property rights are reserved.

License to use Website

- You may view, download for caching purposes only, and print pages from the website, provided that:
- You must not republish material from this website (including republication on another website), or reproduce or store material from this website in any public or private electronic retrieval system;
- You must not reproduce, duplicate, copy, sell, resell, visit, or otherwise exploit our website or material on our website for a commercial purpose, without our express written consent.

Limitations of Liability

The information on this website is provided free-of-charge, and you acknowledge that it would be unreasonable to hold us liable in respect of this website and the information on this website. Whilst we endeavour to ensure that the information on this website is correct, we do not warrant its completeness or accuracy; nor do we not commit to ensuring that the website remains available or that the material on this website is kept up-to-date. To the maximum extent permitted by applicable law we exclude all representations, warranties and conditions (including, without limitation, the conditions implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill). Our liability is limited and excluded to the maximum extent permitted under applicable law. We will not be liable for any direct, indirect or consequential loss or damage arising under this disclaimer or in connection with our website, whether arising in tort, contract, or otherwise - including, without limitation, any loss of profit, contracts, business, goodwill, reputation, data, income, revenue or anticipated savings. However, nothing in this disclaimer shall exclude or limit our liability for fraud, for death or personal injury caused by our negligence, or for any other liability which cannot be excluded or limited under applicable law. Variation We may revise this disclaimer from time-to-time. Please check this page regularly to ensure you are familiar with the current version. Entire agreement This disclaimer constitutes the entire agreement between you and us in relation to your use of our website, and supersedes all previous agreements in respect of your use of this website. Law and jurisdiction

This notice will be governed by and construed in accordance with English law, and any disputes relating to this notice shall be subject to the exclusive jurisdiction of the courts of England

END OF COMPUTING POLICY

Date of Next Full Review: Spring 2028

Head Teacher:_____ **Chair of Governors:**_____

Computing Leader:_____