ONLINE SAFETY POLICY

A Safeguarding Policy

March 2026

Hollyfield Primary School

…a place where everyone matters

Version:	March 2026
Ratified by the Governing Body:	18 March 2026
Signed by the Governing Body:	
To be reviewed (annually):	March 2027

Contents

Appendices (forms)

1. Introduction

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. Computer skills are vital to access life-long learning and employment; indeed ICT and Computing is now seen as an essential life-skill.

Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all sectors of society. This brings young people into contact with a wide variety of influences, some of which, as in life generally, may be unsuitable. This policy will outline how the staff, pupils and Governors at Hollyfield Primary School will adopt strategies for the safe and responsible use of the internet.

The Internet is an open communications channel, available to all. Applications such as the Web, email and chat rooms along with the increase in mobile technologies that we now see in everyday life such as mobile phones, iPad's, Tablets, PC's, Smart Devices all transmit information over the Internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. Live Streaming is becoming ever popular and this in itself can pose risks for internet users. Whilst risks are there these features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be more restricted elsewhere. Increasingly common too, are the issues surrounding Radicalisation & Extremism which school treats with the upmost importance. Sadly, e-mail and chat communication can provide opportunities for adults to make contact with children for inappropriate reasons. In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

Hollyfield Primary will provide Online Safety guidance to parents at all workshops that take place in school. Online Safety tips will be published in weekly newsletters and we will utilise the CEOP Ambassadors in the LTE to deliver up to date content.

2. Safeguarding

In safeguarding our pupils, we need to educate them about the benefits, risks and responsibilities of using information technology. We can quite easily block certain technologies or prevent access to particular websites. Is this educating our pupils? In the home, it is unlikely that parents would have safety and security features such as a firewall or strict filtering systems to prevent children accessing inappropriate content. With the sound advice we provide our pupils in school, we will not simply prevent access but teach them about the roles and responsibility that they have in using them and how to use them safely. By following the schools Acceptable Use Policy (AUP) individuals throughout our school will understand the responsibility that they play in keeping everyone safe while using Information Technology.

The Online Safety Policy will be used in conjunction with other mandatory school policies: child protection, health and safety, home–school agreements, Privacy Notices and behaviour policies including the anti-bullying and Data Protection Policy,

In order for us to work with our pupils and for the policy to work effectively we will need to look at a no blame culture where we accept that at times even the most innocent of web searches could

return some inappropriate material. Pupils need to be confident in that reporting such incidents to an adult; they will be supported and not blamed.

Resources used by pupils in school will be carefully chosen by the teacher and determined by curriculum policies. Use of the Internet, by its nature, will provide access to information which has not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times, they will be able to move beyond these, to sites unfamiliar to the teacher.

Staff are to use their class cameras or iPads to take photographs and the internal school telephone system to make and receive necessary phone calls. Staff may need to access mobile phones for Multi Factor Authentication (MFA) to some school systems. Mobile phones should only be used for authentication purposes. If staff wish to check their mobile phones during the working day they must do so during designated break times and away from children; where possible mobile phones should be used in staff only areas. (There will however be a number of staff who have mobile phones and use these during the day for communication across the site, LTE or to enhance safeguarding.)

We would not expect parents or visitors to use their mobile phones, or other similar devices, whilst visiting our school except for during special occasions where videoing and photographing of their own children has been agreed. Posters informing visitors that school is a 'mobile free zone' may be displayed around school.

The problems and issues surrounding online safety concern all schools. Whilst some of the media interest in this subject is hype, there is genuine cause for concern that children might access unsuitable material either accidentally or deliberately.

The purpose of this policy is to:

- Establish the ground rules we have in school for using the Internet
- Describe how these fit into the wider context of our discipline and PSE policies
- Demonstrate the methods used to protect the children from sites containing pornography, racist or politically extreme views and violence.

The school believes that the benefits to pupils from access to the resources of the Internet, far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians.

We feel that the best recipe for success lies in a combination of site-filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

Parents will be sent an explanatory letter and the rules which form our Internet Access Agreement (See Appendix A) This can be seen as an extension to the Home School Agreement.

3 . Using the Internet for Education

The benefits include:

- access to a wide variety of educational resources including libraries, art galleries and museums

- rapid and cost effective world-wide communication
- gaining an understanding of people and cultures around the globe
- staff professional development through access to new curriculum materials, experts' knowledge and practice
- exchange of curriculum and administration data with Local Authority/Department for Education and Skills
- social and leisure use
- greatly increased skills in Literacy, particularly in being able to read and appraise
- critically and then communicate what is important to others.

The school intends to teach pupils about the vast information resources available on the Internet, using it as a planned part of many lessons.

All staff will review and evaluate resources available on web sites appropriate to the age range and ability of the pupils being taught and disseminate this information.

Initially the pupils may be restricted to sites which have been reviewed and selected for content. They may be given tasks to perform using a specific group of web sites.

Pupils will have the opportunity to exchange information via email. They will be issued with a school email address. They will be taught how to use the address book, how to attach files to an email and how to follow conventions of politeness. Rules can be added to email that means that pupils cannot send or receive emails via external contacts and/or that emails are moderated by the class teacher before they are sent to the intended recipient. This will be discussed and configured with our IT Support team before pupils are issued with email accounts.

As pupils gain experience, they will be taught how to use searching techniques to locate and specific information for themselves. Comparisons will be made between researching from different sources of information, (CD Rom, books, WWW). We hope that pupils will learn to decide when it is appropriate to use the Internet, as opposed to other sources of information, in terms of: the time taken; the amount of information found; the usefulness and reliability of information located.

At times, information, such as text, photos etc may be "downloaded" from the Internet for use in pupils' presentations. Tasks will be set to encourage pupils to view web sites and information with a critical eye.

4. Pupils' Access to the Internet

Hollyfield Primary School will use a filtered Internet Service, which will minimise the chances of pupils encountering undesirable material. This filtering service is managed by SurfProtect filtering and our ISP is EXA Networks.

- Hollyfield Primary School will only allow children to use the Internet when there is a responsible adult present to supervise. Pupils will be directed to websites by staff that will have checked out the suitability beforehand. If a URL is encountered that is deemed to be inappropriate then the member of staff should report this to the ICT Manager who will investigate and refer to the appropriate authorities for the URL to be added to the list of blocked sites.
- HTTPS INSPECTION. Google and many other search engines and websites now offer secure connections using HTTPS. A security certificate will be deployed across our network allowing Surfprotect filters to successfully decrypt and encrypt packets on the network via websites hosted

with https. Visitors, and users of the guest network will accept that this certificate may be installed on their device.

Members of staff will be aware of the potential for misuse, and will be responsible for reminding pupils of responsible Internet use, all users will need to "Accept" the schools AUP to logon to desktop & laptops in school. Failure to accept the AUP will force the users to log off. (see Appendix A).

- Teachers and System Administrators have the power to lock access to pupils' emails and other Internet related files and will check these on a regular basis to ensure expectations of behaviour are being met. Some emails deemed to be SPAM, Malicious, containing profanity or certain file types are filtered using the Microsoft Office 365 platform. Like all filtering systems no one system is 100% accurate and so pupils will be reminded of their responsibility should they receive anything inappropriate or that causes them distress so that this can be investigated and where necessary tools put in place to prevent any recurrence. Users will be able to request emails are released if they believe they are being withheld in error. These email types will be automatically deleted after 14 days.

"Schools have a responsibility to educate young people and provide a safe learning environment. Increasingly, ICT is used as an integral part of teaching and learning, and evidence shows that it can have many important benefits. Schools, therefore, must also play a special role in educating children and young people about the safe use of the Internet and related technologies". **BECTA BECTA has been replaced by NAACE**

To maintain personal safety pupils and staff at Hollyfield, will work to the SMART rules.

S – Safe
M – Meeting
A – Accepting
R – Reliable
T – Tell

They will not:

- Post personal contact information about themselves or other people. Personal information includes names, address and telephone numbers etc.
- Attempt to gain unauthorised access to any computer, user account, files or folders which is beyond their security levels.
- Download programs or files without seeking permission from the ICT Manager, ICT co-ordinator or supervising member of staff
- Be allowed access to public or unregulated chat rooms.
- Use Personal USB or external hard disks to transfer data to and from the school network without prior agreement with the Network Manager and only once those devices have been virus checked.

5. Expectations of Pupils using the Internet

- All pupils are expected to read and agree the Internet Agreement.
  We expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.

Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the Service Provider can block further access to the site.

- Pupils are expected not to use any inappropriate language in their email communications and contact only people they know or those the teacher has approved. They will be taught the rules of etiquette in email and are expected to follow them.

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

- Pupils should not access other people's files unless permission has been given.

- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.

- No program files may be downloaded to the computer from the Internet. This is to prevent corruption of data and avoid viruses or data loss.

- No programs on memory stick, disc or CD Rom should be brought in from home for use in school. This is for both data protection and security reasons. A child needing to take material home can use their personal workspace. Pupil access to USB drives will be blocked to minimise the risk of cyber attacks and Ransomware. USB drives may be allowed in special circumstances and by prior arrangement with class teachers and IT support staff.

- No personal information such as phone numbers and addresses should be given out and no personal arrangements to meet anyone will be made on the internet.

- Pupils choosing not to comply with these expectations will be warned, and subsequently, if further instances occur, will be denied access to Internet resources. They will also come under the general discipline procedures of the school which comprises an escalating set of measures including a letter to parents and withdrawal of privileges.

6. School Web Site Guidelines

A web site can celebrate good work, promote the school, and publish resources for projects and homework, and link to other good sites of interest.

- Information published will be accurate as at date of publish, and any inaccuracies that may occur will be corrected as soon as is possible.
- Where photos of pupils are to be uploaded then agreement will be made with parents and names will not be published. We will adopt a "photo, no name – name, no photo" approach and where possible only forenames should be used to minimise identification.
- Files uploaded will not refer to names. E.g. A photo of Joe Bloggs will not have a filename joebloggs.jpg.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.
- Group photos will not contain a names list.
- Display will be of the highest quality and reflect the status of the school

- Home information and e-mail identities will not be included only the point of contact to the school i.e. phone number, school address and all emails will be submittable through on site forms, no email address will be posted on the website.

7. Information System Security

- Virus detections will be dealt with promptly and where staff laptops are affected staff will be notified immediately and asked to bring the laptop into school ASAP for quarantine.
- All workstations and laptops in school will be updated with Microsoft critical updates each half term or in the case of an urgent update this will be completed at the earliest opportunity.
- School security settings for the network, user accounts and folder structures will be reviewed regularly.
- Any suspected access or security issue will be reported to the head teacher or the ICT Manager at the earliest possible time.

8. Password Policy

Passwords will be in place for accessing the school network and associated systems.

EYFS will access the network using a generic class login. This will allow for a more productive lesson and give younger pupils the opportunity to login with a simple login name.

KS1 and KS2 pupils will be allocated individual usernames and passwords. Passwords cannot be changed by pupils allowing staff to access a secure list in the event of a pupil forgetting their credentials.

Staff will access systems with their own account details and passwords. Passwords can be changed by staff at anytime for security reasons. Strong passwords are encouraged to minimise the risk of accounts being compromised. We will not force periodic changes to passwords where possible as this can result in minimal changes such as adding numeric values to the end of passwords or can encourage users to write down frequent passwords thus increasing the risk of passwords falling into the wrong hands. Some of our system do however force changes and this cannot be changed.

9. Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars if using social networking sites outside of school.
- Staff are expected to be professional at all times. Anything they post online via social networking sites could reflect on the school and them as an individual.
- All staff are expected to use Social Media responsibly and follow guidance set out in the "LTE Social Media Policy".

10. Staff Laptops & iPads

- Teaching staff are allocated a laptop and iPad for PPA purposes.
- The devices can be connected to the internet out of school but must be used for school business.
- Staff laptops will be returned to the school ICT Manager/technician regularly for critical updates and software installations.
- Any loss or damage will be reported immediately.

11. Personal Data and Data Protection

- Personal Data will be stored securely and will be restricted to staff members who need the information.
- Confidential data will be stored on the staff shared area to which only staff will have access.
- All staff will have a user account and understand the importance of a secure and strong password.
- Access to the school Management Information System (MIS) and financial accounts information will be restricted by role.
- Staff will only have access to MIS systems if their role requires it.
- MIS access will be restricted for all users allowing them to view the data to which they are entitled.
- Access to the Admin network will be restricted for all users other than Admin staff.
- Personal Data will not be stored on shared drives to which children have access.
- Photos and video footage of pupils will be stored to allocated locations solely for photos and video.
- Children's or Staff personal data will not be transferred offsite by means of USB/flash drives unless specific permission is granted. If this data is necessary then the media MUST be encrypted to prevent unlawful access or any data loss or breaches under GDPR.
- Data that can identify an individual should not be stored on staff laptops or offsite, and staff should be aware of the responsibility they have in minimising the risk for this data to be obtained by third parties.
- Staff may be issued with an encrypted memory pen for data storage but personal data is not endorsed.

12. Handling Online Safety Complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint of staff misuse will be reported to and dealt with by the head teacher and SLT misuse by a designated Governor.
- Complaints of a child protection nature must be dealt with in accordance to the school's child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Complaints of internet misuse at the before and after school provision will be dealt with by the Organiser.
- Misuse by members of the Senior Leadership Team will be dealt with by the Head Teacher

13. Plagiarism and Copyright Infringement

Staff need to be aware of copyright laws with regards to information on the World Wide Web. Government websites are generally free from copyright. However, all other websites are copy written. It is always good manners to send an email to the owner of the materials to confirm that

they are willing to allow copying of pages of information. Projection or screen viewing of resources is permitted.

Staff are encouraged to look around for free information and use visual projection when accessing resources from the Internet.

14. Registration

Sims allows class teachers to take online registration enabling instant and up to date records for office staff on the attendance of pupils. The systems allow access to personal data of pupils such as attendance information, emergency contact details and address information. It is therefore vitally important that when staff use this system they logout once registration is complete. Staff must never allow children to access the system and must never divulge the username/password to pupils. If a staff member suspects the password has been compromised they will log a helpdesk call for the IT team to reset their password as soon as possible. This packages will be closed when not in use and the class teacher or user will ensure the PC is locked when unattended.

15. Useful Web Links

www.childnet.com
www.thinkuknow.com
www.thegrid.org.uk/eservices/safety
www.naace.co.uk
www.ceop.police.uk

16. Acceptable Use Policy (AUP) – Pupil Version

All pupils and their parents / guardians will be asked to read and sign an agreement covering the expectations we have of pupils using the Internet in school. Acceptable Use Policies will appear at login for users to read and agree to. The AUP will need to be agreed to allow successful logon to computers. If a user fails to accept the AUP they will be automatically logged off the system and returned to a logon screen.

See Appendix A for the Parent Letter
See Appendix B for the Pupil AUP

17. Acceptable Use Policy (AUP) – Staff Version

All staff and adults using computers in school will be required to agree to the staff AUP. As with the pupil AUP, users will be given an opportunity to agree to the AUP at logon. Failure to agree will force the computer to log the user off and the machine will return to a login screen.

See Appendix C for the Staff AUP

18. Pupils' Mobile Phones

At Hollyfield Primary School, pupils are not permitted to have mobile phones at school or on trips. However, we do understand that parents of children in Years 5 and 6 may wish them to have a mobile phone if they are walking to and from school without an adult. In this instance, children must turn their phone off once they reach school gates. Children must hand

their phone into their class teacher who will ensure that it is kept in a locked cabinet in the school office until the end of the school day. If a child is found to be using a mobile phone during the school day without prior consent, then it will be confiscated and parents will be informed.

Appendix A

Dear Parents/Carers

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, we provide supervised access to the Internet. We believe that use of the World Wide Web and email is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible Internet Use with your child and sign and return the consent form so that your child may use the Internet at school.

Our school Internet provider operates a filtering system that restricts access to inappropriate materials.

The school has prepared an Internet Access Policy which is intended to help us make the most of the opportunities that the Internet offers whilst minimising the possible risks.

Should you wish to discuss any aspect of the Internet, please do not hesitate to contact me.

Yours sincerely

Appendix B

Acceptable Use Policy – Pupil Version

I want to feel happy and safe all the time.

I agree that I will:

- always keep my passwords a secret
- not look at or delete other people's work,..
- not bring my own memory sticks or other portable storage devices into school without asking my teacher first.
- only use my school email
- only email people that my teacher allows me to.
- only send messages that are sensible and polite.
- show my teacher if I get a nasty message
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable on the internet
- make sure all messages I send are polite
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family or pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger

Anything I do on the computer may be seen by someone else.

I know that if I break these rules, my access to computer may be restricted.

I am aware of the CEOP report button and know when to use it. Do we use this??

Pupil Name…… Date…… Signed……

Parent/Guardian

Name…… Date…… Signed……

Appendix C

Staff User Agreement

To ensure all staff fully understand their responsibilities regarding ICT use, we require them to sign this Acceptable Use Agreement.

- I acknowledge that the school network is the property of Hollyfield Primary School, and I agree to use it in a manner consistent with my professional role.
- I understand that the school's ICT systems are not to be used for personal purposes unless I have explicit permission from the Headteacher.
- I recognise that the following actions are strictly prohibited. Any staff member or individual using Hollyfield Primary School's ICT infrastructure who breaches or attempts to breach this policy will face disciplinary action in line with the school's procedures, which could include criminal prosecution or dismissal. Prohibited actions include accessing, searching for, storing, downloading, or forwarding any materials—whether text, images, audio, or data—that are:
    - Obscene
    - Offensive
    - Sexual in nature
    - Politically offensive
    - Likely to bring the school, Birmingham City Council, or the individual into disrepute
    - Participating in newsgroups, chat rooms, or similar forums
    - Using the network to run a private business, such as selling or advertising
    - Violating copyright laws (including images, text, music, or video in any format)
    - Using web-based email services other than those provided by the school
    - Attempting to bypass network or computer security measures
- I understand and agree that mobile phones must not be used during the school day when children are present. Specifically:
    - I will use class iPads for taking photographs.
    - I will use the internal school telephone system for necessary calls unless otherwise authorised by the Headteacher.
    - If I need to check my mobile phone during working hours, I will do so only during designated breaks, away from children, and in staff-only areas.
- I accept that the school will monitor network and internet use to ensure compliance with this policy.
- I will respect the security of ICT systems and understand that it is a criminal offence to use computers for purposes not authorised by the school.
- I will not install any software or hardware without prior approval.
- All portable media such as memory sticks and flash drives must be encrypted.
- I will not share or disclose personal or sensitive information with third parties without the knowledge and approval of the Data Protection Officer (DPO).
- I will keep all passwords and login credentials confidential, except where disclosure is necessary to authorised staff responsible for system maintenance.
- I will take all reasonable precautions to protect data and equipment taken off-site and report any loss or security breaches immediately to the DPO and Headteacher.

- I will not allow family members or non-school personnel to use school computing equipment taken home.
- I will promptly report any concerns or incidents to the school's Designated Child Protection Officer.
- I will ensure all electronic communications with pupils remain professional and appropriate, avoiding any possibility of misinterpretation.
- I will actively promote online safety with the pupils I work with, helping them to develop responsible attitudes towards ICT use.
- Disposal of school software and hardware will only be conducted in accordance with the IT disposal policy and must be authorised by the E-Learning Manager, IT technician, and Bursar. Any unauthorised disposal may be considered theft.
- I will respect copyright and intellectual property rights at all times.

The school reserves the right to monitor use of its computer systems, including website access, email interception and the removal of inappropriate materials, particularly if there is suspicion of unauthorised or criminal use, or if unlawful content is stored on the systems.

Signed…… Capitals……

Date …….