Online Safety Policy

The John Harrox Primary School

Approved by:	[Governing Body]	**Date:** [18/10/2023]
Last reviewed on:	[18/10/2023]	
Next review due by:	[September 2024]	

The John Harrox Primary School
Online Safety Policy
September 2023

Policy Statement

For clarity, the online safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body and parents.

Safeguarding is a serious matter; at The John Harrox Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as online safety, is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an online safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on The John Harrox Primary School website; upon review all members of staff will sign as read and understood both the online safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Students Acceptable Use Policy will be sent home with students as they start school with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Headteacher Name: Signed:

Chair of Governors: Signed:

Review Date: September 2023 Next Review: September 2024

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Seek assurance to ensure suitable filtering and monitoring systems are embedded into the school's ICT infrastructure.

- Appoint one governor to have overall responsibility for the governance of online safety at the school who will:

    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

    The online safety governor is: Josh Adams

Designated Safeguarding Lead

Reporting to the governing body, the Designated Safeguarding lead has overall responsibility for online safety within our school. The day-to-day management of this will be delegated to a member of staff, the online safety Officer, as indicated below.

The Designated Safeguarding lead will ensure that:

- Online safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- That appropriate filtering and monitoring systems and processes are in place and that consideration is taken for those who are at greater risk of harm and how often they access the IT system.
- The designated online safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All online safety incidents are dealt with promptly and appropriately.
- Retain responsibility for the online safety incident log (CPOMS); ensure staff know what to report and ensure the appropriate audit trail.

Online Safety Officer

The day-to-day duty of Online Safety Officer is devolved to Chloe Wicks
The Online Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize herself with the latest research and available resources for school and home use.

- Review this policy regularly and bring any matters to the attention of the Headteacher and Designated Safeguarding lead.
- Advise the Headteacher, Designated Safeguarding lead, and governing body on all online safety matters.
- Engage with parents and the school community on online safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Ensure any technical online safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with Ark (ICT Technical Support.)

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any online safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the online safety officer and Designated Safeguarding lead.
    - Usernames and passwords are applied correctly to all users, except EYFS. Passwords for staff will be a minimum of 8 characters.
    - The IT System Administrator password is to be changed on a monthly (30 day) basis.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood, it should be brought to the attention of the Headteacher.
- Their usernames are predetermined by the school using the system of 'firstname.surname' e.g. Chloe.Wicks and passwords are unique to them and kept private. Ipads should have at least a 6 digit code.
- Any online safety incident is reported to the Designated Safeguarding lead (and an online safety Incident report is made on CPoms), or in her absence to the online safety officer. If you are unsure, the matter is to be raised with the online safety Officer or the Headteacher to make a decision.
- All devices that carry sensitive data are encrypted and password protected. Multifactor authentication is active for staff for additional protection.
- USB pen drives are not used in school.
- Any sensitive data (including children's names) sent by email should be encrypted by putting 'encryptmail' in the subject line of the email. Emails containing sensitive data should not be sent to any personal email addresses.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

Online safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly, all students will be fully aware how they can report areas of concern whilst at school or outside of school. Outside agencies will also be used where appropriate to provide additional online safety teaching to the children.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through for example, parents evenings, school newsletters, curriculum evenings and the John Harrox Primary School website, the school will keep parents up to date with new and emerging online safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Technology

The John Harrox Primary School uses a range of devices including PC's, laptops, Ipads and a Mac. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering and Monitoring – we use the highest quality filtering and monitoring systems to mitigate the risks of our children's online safety. The John Harrox primary school uses ***Securly***, as its filtering system, employing a continuously updated series of keywords and watchwords to filter the content of the internet from any of the machines within the school system. This prevents unauthorized access to illegal websites as well as inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. Reports can be run against each child's user to determine which websites they have gained access to and alerts for specific categories (E.g. Pornography) are set up to inform the designated safeguarding lead if someone has attempted to access a website of this nature.

All of the children's iPads are a part of the school's ***Senso*** monitoring program. For each child to access the internet through Senso, they submit their personal details (first name and surname) before they can begin their digital exploring. The system monitors keyboard entries and reports key words and watch words as they are typed on any child's keyboard. This provides real time and highly effective monitoring of all users on the school system. In the case of a key word being searched, an email is immediately sent to the designated safeguarding lead, indicating the word or phrase used and from which user it came from, allowing for appropriate action to be taken.

The Online Safety Officer, IT Support and the Designated Safeguarding Lead are responsible for ensuring that the filtering and monitoring systems in place are appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – we use the built in Office 365 software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing messages.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as a laptop or an ipad) is to be brought to the attention of the Headteacher immediately. The designated safeguarding lead will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office. *(Note: Encryption does not mean password protected.)*

Passwords – all staff and students, except EYFS, will be unable to access any device without a unique username and password. Staff will have their own unique passwords which will change if there has been a compromise. Staff also have Multifactor Authentication for their accounts.
Staff ipads should be password protected with at least a 6 digit code.
Note: Student Ipad's should not be password protected.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out and will report to the Headteacher if there are any concerns.

All filtering and monitoring systems are regularly reviewed to ensure their effectiveness through liaising with Ark technical support, such as the fortnightly technician visit to school.

Use of Technology in school

As staff at the John Harrox Primary School we are responsible for ensuring that technology is used in a responsible and respectful manner by everyone in school. We do this by adhering to the following procedures. These also form part of the acceptable use policy which is signed by staff on an annual basis. Pupils also sign an acceptable use policy on a yearly basis.

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this online safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.
Staff email addresses are set up in the following way firstname.surname@johnharrox.lincs.sch.uk – ie chloe.wicks@johnharrox.lincs.sch.uk
Students are permitted to use the school email system whilst being closely supervised by a teacher. At the present time email addresses are NOT anonymised and children should only use them for internal emails. Children's email address are made up of their first name and surname, e.g. firstname.surname@johnharrox.lincs.sch.uk

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy, and is re-iterated here for clarity. All parents must sign a photo/video release slip; non-return of the permission slip will not be assumed as acceptance. The Head and Governors have the responsibility to decide if photography and videoing of school performances is permitted. Parents and carers can use photographs and videos taken at a school event for their own personal use only. Such photographs and videos cannot be passed on or sold or put on the web/internet without consent. Staff are not allowed their mobile phones or personal cameras out in the classroom while children are in the building. School equipment is provided to take photos and videos of the children during educational activities.

Mobile phones – Whilst mobile devices are a source of fun, entertainment, communication, and education, we know that some adults and young people may use these technologies to harm young people. The harm might range from hurtful and abusive messages directed at them, inappropriate and harmful content, to enticing young people to engage in sexually harmful conversations, video calls, indecent image sharing or face-to-face meetings. Through our online safety lessons and other curriculum lessons, such as PSHE (Jigsaw), we will support the children with how to maintain their own safety as well as how to summon help if they are concerned.
Whilst at the John Harrox Primary School we are aware of the increasing use of mobile phones in primary school aged children, we do not permit the use of mobile phones in school, and they should not be brought on to school grounds. In circumstances where a parent/carer has requested that their child brings a mobile phone to school, it is to be handed into the office in the morning and collected at the end of the school day.

Social Media – there are many social media available; The John Harrox Primary School is fully supportive of social media as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. Most social media are only available for people who are over the age of 13, therefore they are inappropriate for children to use in school. Our school IT filtering software prevents the children from accessing any social media accounts. We will work with young people on how to maintain their own safety and how to summon help if they are concerned about what they see online. Some young people will undoubtedly be chatting through apps or social media at home and parents are encouraged to consider measures to keep their young people safe.
Should staff wish to use a social media site with their class, permission must first be sought via the online safety Officer who will advise the Headteacher and designated safeguarding lead before a decision to be made. Any new service will be risk assessed before its use is permitted.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name is only to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed.

Incidents - Any online safety incident is to be brought to the immediate attention of the designated safeguarding lead and the online safety officer. The designated safeguarding lead and online safety Officer will assist in taking the appropriate action to deal with the incident and will assist in filling out an incident log on CPoms.

Bullying - Online bullying should be treated like any other form of bullying and the school behaviour policy should be followed for online bullying, Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Vulnerable children – The John Harrox Primary School is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or children with English as an additional language (EAL) and children experiencing trauma or loss. We will ensure that differentiated and ability appropriate online safety education, access, monitoring and support is provided to vulnerable pupils.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. The introduction of Project Evolve to support the teaching of Online Safety will support staff with the subject knowledge required to effectively teach this aspect of the curriculum.

Whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning. Online safety for students is embedded into the computing curriculum and in other cross curricular subjects where appropriate; such as through the teaching of our PSHE scheme (Jigsaw), which has specific topics regarding relationships and positive self image. The Education For a Connected World Framework creates the basis for our online safety teaching within school, focusing on developing the children's awareness of:

- Self-image & identity
- Online relationships
- Online reputation
- Copyright and Ownership
- Online bullying
- Managing online information
- Health, well-being and lifestyle
- Privacy and security

The school uses resources from Project Evolve to teach online safety across the school on a yearly basis. As well as using outside agencies to support the teaching of online safety in Year 5/6.

As well as the programme of training, we will establish further training or lessons as necessary in response to any incidents.

The online safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher, designated safeguarding lead and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Children's independent use of ICT - To ensure the safeguarding of the children, they will only be allowed to use internet enabled technology (desktop PC and iPads) when being supervised by a member of staff. Children are not allowed to be unaccompanied in the ICT suite or Ipads in the classroom. Pupils should be guided when engaged in learning activities involving online technology, supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright.

Use of iPad's in school

Home use - The school has a bank of 60 iPads. When they are not being used they must be placed in their charging trolley. IPads are a resource to promote learning across the school and should not be taken home for personal use. Teaching staff have an iPad to support planning and assessment which can be used at home to support school related activities. Children are not allowed to take the Ipads home for personal or school use.

Purchasing of Apps – The purchasing of Apps in school will be made by the computing coordinator or the Headteacher. These will be purchased through The Volume Purchase Programme (VPP). The VPP allows educational institutions to purchase iOS apps and books in volume and distribute them to all the ipads in school.

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the online safety Policy. Once you have read and understood both you must sign this policy sheet..

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an online safety incident, reported to the online safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the online safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks, unless they are family members/friends.

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional (remember to be aware of your personal digital footprint). Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support. Supply teachers are able to use the supply log in.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device is encrypted and password protected. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal devices (including camera phones) – Personal devices should not be used or be visible in the presence of pupils.

Viruses and other malware - any virus outbreaks are to be reported to Ark as soon as it is practical to do so, along with the name of the virus (if known) and the actions taken by the school.

Online safety – like health and safety, online safety is the responsibility of everyone to everyone. As such you will promote positive online safety messages in all use of ICT whether you are with other members of staff or with students.

NAME :

SIGNATURE : **DATE :**

Acceptable Use Policy – Students

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting. If I accidently find anything like this, I will tell my teacher immediately.

I Promise – to show respect for the work that other people have done and not use their work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my username and password with anybody. If I forget my username or password, I will let my teacher know.

I will not – use other people's usernames.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I will – only open my own work and files.

I understand – that some people on the Internet are not who they say they are, and some people can be unkind. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

I will - be responsible for my behaviour when using ICT because I know these rules are to keep me safe.

Child's Name:…… Class……

Signed (Students Year 3 and above) : …… Date……

Signed (Parent/Carer)…… Date……