John Hunt Academy

E-Safety Policy

Approved by:	Mrs A Good & Miss L Devlin	Date: 13/03/2026
Last reviewed on:	13/03/2026	
Next review due by:	13/03/2027	

Contents

Please note that the version of this document contained at https://www.johnhuntprimary.co.uk is the only version that is maintained. Any printed copies should therefore be viewed as 'uncontrolled' and as such, may not necessarily contain the latest updates and amendments.

Equality

SHINE Multi Academy Trust (SHINE) and its academies are committed to promoting equal opportunities and all stakeholders will receive equal treatment regardless of age, disability, gender reassignment, marital or civil partner status, pregnancy or maternity, race, colour, nationality, ethnic or national origin, religion or belief, sex or sexual orientation (protected characteristics).

Introduction

At John Hunt Academy, we are committed to ensuring that children learn how to use computers, ICT and modern technologies safely so that they:

- Are able to use ICT safely to support their learning in school
- Know how to use a range of ICT equipment safely
- Are able to use ICT and modern technologies outside school in a safe manner, including using ICT as a tool for communication
- Are prepared for the constant changes in the world of technology and understand how to use new and emerging technologies in a safe manner
- Know what to do if they feel unsafe when it comes to using technology and ICT

This policy outlines the steps the school takes to protect children from harm when using ICT and also how the school proactively encourages children to develop a safe approach to using ICT whether in school or at home.

The Law

Our E-Safety Policy has been written by the school, using government guidance. The Policy is part of the school's Strategic Development Plan and related to other policies including Positive Learning, Safeguarding and Data Protection policies.

As legislation is often amended and new regulations introduced the references made in this policy may be superseded. For an up-to-date list of legislation applying to schools please refer to the Department for Education website at:

https://www.gov.uk/government/publications/teaching-online
https://www.gov.uk/government/publications/teaching-online-safety-in-schoolssafety-in-schools

Roles and Responsibilities

The Headteacher, alongside SLT and the Computing Lead

- Ensure the policy is implemented, communicated and compliance with the policy is monitored
- Ensure staff training in e-safety is provided and updated annually as part of safeguarding training, including contextualised safeguarding
- Ensure immediate action is always taken if any risks or dangers are identified i.e. reporting of inappropriate websites
- Ensure that all reported incidents of cyber bullying and contextualised safeguarding reports are investigated

- Ensure appropriate web filtering software is used to protect users from potentially damaging/offensive material with regular reports to SLT and governors
- Pupils are expected to take an active part in lessons and activities to support their understanding and confidence in dealing with online safety issues, both at home and school.

Teachers and Staff will:

- Keep passwords private and only use their own login details, which are stored securely
- Monitor and supervise pupils' internet usage and use of other IT resources
- Adhere to the Acceptable Use Agreement
- Promote e-safety and teach e-safety units as part of computing curriculum
- Engage in e-safety training, including updates on contextualised safeguarding
- Only download attachments/material onto the school system if they are from a trusted source
- When capturing images, videos or sound clips of children, only use school cameras or recording devices

It is essential that pupils, parents/carers and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of staff members and the reputation of the school and the County Council are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

Governors will:

- Ensure that the school is implementing this policy effectively
- Adhere to the acceptable use agreement when in school
- Have due regard for the importance of e-safety in school and receive regular NSPCC newsletters

Teaching and Learning

The school will actively teach E-safety at an age-appropriate level.

E-safety will also be embedded throughout learning whenever children are using ICT in other lessons. The purpose of Internet use in school is to raise educational standards, promote pupil achievement, support the professional work of staff and enhance the school's management functions. Internet use is part of the statutory curriculum and a necessary tool for learning. The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use benefits education by providing:

- access to world-wide educational resources including museums and art galleries educational and cultural exchanges between pupils world-wide
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across networks of schools, support services and professional associations

- improved access to technical support including remote management of networks and automatic system updates
- access to learning wherever and whenever convenient

Pupils will be taught what internet use is acceptable and what is not and given clear objectives for Internet use. They will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. John Hunt Academy will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. The school will provide opportunities within a range of curriculum areas to teach online safety. Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the online safety curriculum.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Monitoring Safe and Secure Systems

Internet access is regulated by ATOM: FORTIGATE, supplied filtered broadband connection which blocks access to unsuitable websites. Antivirus software has been installed on all computers and school will ensure this is maintained. Staff passwords are changed regularly and must be strong passwords. Staff take responsibility for safeguarding confidential data saved to laptops, i.e. use of strong passwords.

The school does not allow personal devices such as USBs or any other external devices. Staff with access to the ICT systems containing confidential and personal data are to ensure that such data is properly protected at all times. Teaching staff have remote access to the school server. This reduces the need for portable data storage and therefore increases security. Remote access is fully password protected.

Safe use of the Internet and Web Filtering

- All staff and pupils will have access to the internet through the school's network
- All staff, volunteers who have use of the school's IT equipment, must read and sign the Staff Acceptable Use Agreement.
- If a site containing inappropriate material is encountered, children must report it to an adult who will report it to the Headteacher to pass to ATOM: FORTIGATE through email or telephone if it is not initially blocked.
- If an adult finds a site that they consider unsuitable they should report it to the Headteacher, SLT or Computing lead.

The Use of Email

All teaching and support staff are provided with a school email address. Staff should use this address when sending work-related emails. All emails should be professional in nature and staff should be aware that all emails can be retrieved at a later date should this be necessary. Staff emails should never be used to forward 'chain' or 'junk' email.

The School Website

The school web site complies with statutory DFE requirements

Images that include pupils will be selected carefully and only used if parents have given permission for such images to be posted on line.

Social Networking, Social Media and Personal Publishing (Blogging)

The school recognises that it has a duty to help keep children safe when they are accessing such sites at home, and to this end the school will cover such issues within the curriculum. Pupils will not access social networking sites, e.g Facebook, Instagram or Snapchat in school. They will be taught about how to stay safe when using such sites at home.

Staff Private Use of Social Media

- No reference should be made in social media to students / pupils, parents /carers / school staff or issues / situations related to the school
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- Staff are not permitted to maintain a Social Media relationship with any pupil, current or alumni until such time that the pupil turns 18.

The Use of Cameras, Video and Audio Recording Equipment

Staff may only use the school's photographic or video devices to support school trips and curriculum activities. Photos should only be uploaded to the school system. They should never upload images to the internet unless specific arrangements have been agreed with the Headteacher, Deputy Headteacher, or Assistant Heads, nor circulate them in electronic form outside the school. It is never acceptable to use photographic or video devices in changing rooms or toilets.

Personal Mobile Phones and Mobile Devices

Use of mobiles is discouraged throughout the school, particularly in certain areas. The areas which should be considered most vulnerable include:

- Toilets and changing areas, including where children change for swimming.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

Management of Online Safety Incidents

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions; all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes; support is actively sought from other agencies as needed (i.e. MASH, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school
- Parents/carers are specifically informed of online safety incident involving young people for whom they are responsible
- The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform MASH.

Working in Partnership with Parents

Parents' attention will be drawn to the e-safety policy through the school newsletters, information evenings and on the school website. A partnership approach with parents will be encouraged. Parents will be requested to sign an Acceptable Use Agreement as part of the Home School Agreement on entry to the school.

Protecting School Staff

In order to protect school staff we require that parents do not comment on school issues or staff using social networking sites. Any concerns or complaints should be discussed directly with the school. The school will take action if there is evidence that inappropriate comments about staff have been placed on the internet in a public arena.

Safeguarding – Scope of this Policy

(See also Safeguarding and Behaviour policies)

The Head Teacher to such extent as is reasonable, can 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 cyberbullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the school's Behaviour Management Policy. The school will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Online Bullying

While online bullying is likely to be low level in primary schools the age of pupils making proficient use of technology is ever decreasing. Therefore, the opportunities for pupils to bully or be bullied via technology, such as e-mail, texts or social media platforms, are becoming more frequent. As such, teaching pupils about appropriate behaviours when using technology provides a vital grounding for future use.

Whilst not wanting to provoke unrecognised opportunities in pupils, consideration must be given to suitable teaching and procedures to address any issues of online bullying.

All incidents of online bullying reported to the school will be recorded. Online bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying. Complaints of online bullying will be dealt with by the designated safeguarding leads or the specialist teaching and learning assistant. Any complaint about staff misuse must be referred to the headteacher.

Radicalisation and Extremism Online

We recognise that children / young people can be enticed into radicalisation as they are more vulnerable and susceptible to this. They therefore can be drawn into violence or they can be exposed to the messages of extremist groups by many means especially on line and through social media. The school recognise that social media is increasingly a child's or young person preferred method of communication which can increase their risk to exposure to radicalisation.

We will try and help our pupils to keep safe on line and consider the impact of social media networking sites with additional consideration to the threat of exposure to extremism and radicalisation. We are aware of the increased risk of online radicalisation and how terrorist groups seek to radicalise young people on line.

We will treat any worry or concern that a child or young person in the school may be exposed to possible extremism, extremist ideology and or radicalisation as a Prevent concern. We will use the guidance and assessment as prescribed by John Hunt Academy and SHINE.

Indecent Images

We recognise that this is an increasing safeguarding concern which requires a robust response. We will seek advice from agencies and professionals acknowledging that there are both national and local guidance that we need to adhere to in order to tackle the concerns and work in partnership with our agencies.

We will refer to:

- SHINE's child protection and safeguarding policy https://www.shine-mat.com/pupil-welfare/
- Nottinghamshire safeguarding children partnership
- https://nscp.nottinghamshire.gov.uk/
- http://www.workingtogetheronline.co.uk/

The DfE guidance 2018 on Searching Screening and Confiscation Advice

Communicating the Policy

Online safety rules will be displayed in all classrooms and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers and the school will provide opportunities within a range of curriculum areas to teach online safety. Pupils will also be involved in the annual 'Safer Internet Day' which takes place in February. Members of the school council will look through this policy and recommend any necessary amendments.

To protect all staff and pupils, the school will implement acceptable use policies. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Staff training in safe and responsible Internet use both professionally and personally will be provided every two years with a reminder during the safeguarding update every year.

All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community. All staff will be given a copy of this policy.

Parents/carers' attention will be drawn to the importance of online safety through newsletters home, the school website, the school Facebook page, internet safety assembly and information home. Guidance for parents on online safety will be made available to parents in a variety of formats. Parents/carers will be asked to sign permission slips about the children's use of the Internet, filtering and their child's name, photo and work being used on the school website.

The school website contains useful information and links to sites like Thinkuknow, CEOP and the CBBC Web Stay safe page. We will make this policy available to our parents/carers, to our local community. This Policy will also be made available on the school website.

Related policies

Policy	**Website link**
Acceptable use of IT	School Office
Anti-bullying	https://www.johnhuntprimary.co.uk/policies/
Child Protection and Safeguarding	https://www.johnhuntprimary.co.uk/policies/
Data protection	https://www.shine-mat.com/gdpr/
Equality	http://www.shine-mat.com/pupil-welfare/
Filtering and Monitoring	