ONLINE SAFETY POLICY

Approved by:	Local Governing Body	**Date:** May 2021
Last reviewed on:	June 2021	
Next review due by:	June 2022	

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study. Academies, including free schools, if applicable, add/amend: This policy complies with our funding agreement and articles of association.

3. Roles and Responsibilities

3.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

If applicable, add: The governor who oversees online safety is the Safeguarding Governor.

All governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on Acceptable Use of the school's ICT systems and the internet (appendix 2).

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's DSL [and deputy/deputies] are set out in our Child Protection and Safeguarding Policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Headteacher, Network Manager and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the School Behaviour Policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Headteacher and/or governing board.

This list is not intended to be exhaustive.

3.4 The Network Manager

The Network Manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Liaising with members of the school Pastoral and Safeguarding team to provide information related to misuse of the school system or instances of cyberbullying.
- This list is not intended to be exhaustive.

3.5 All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.

- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2).
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the School Behaviour Policy.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2).
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
    - What are the issues? - UK Safer Internet Centre
    - Hot topics - Childnet International
    - Parent factsheet - Childnet International
    - Healthy relationships – Disrespect Nobody

3.7 Visitors and Members of the Community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum and the safe use of social media and the internet will also be covered in other subjects where relevant.
The introduction of the new Relationships and Sex Education (RSE) curriculum was compulsory from September 2020. Under the new requirement, all schools have to teach Relationships and Sex Education and Health Education in secondary schools.

In Key Stage 3, Pupils Are Taught To:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils In Key Stage 4 Are Taught To:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns.
- By the end of secondary school, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.

The safe use of social media and the internet will also be covered in other subjects where relevant.

Pupils In Both Key Stages Are Taught:

- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail.

5. Educating Parents about Online Safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website, social media or virtual learning environment (VLE). This policy will also be shared with parents.

Online safety will also be covered as appropriate during parents' evenings.
If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.
Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

6. Cyber-Bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the School Behaviour Policy.)

6.2 Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils; as part of the safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- cause harm, and/or;
- disrupt teaching, and/or;
- break any of the school rules.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- delete that material, or;
- retain it as evidence (of a criminal offence or a breach of school discipline), and/or;
- report it to the police.

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 Risk Assessment.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.
Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.
More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils Using Mobile Devices in School

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons.
- Tutor time.
- Clubs before or after school, or any other activities organised by the school.

Any use of mobile devices in school by pupils must be in line with the Acceptable Use Agreement (see appendices 1 and 2).

Any breach of the Acceptable Use Agreement by a pupil may trigger disciplinary action in line with the School Behaviour Policy, which may result in the confiscation of their device.

9. Staff Using Work Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least eight characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date – always install the latest updates.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Network Manager.

10. How the School Will Respond To Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the [Staff Disciplinary Procedures/Staff Code of Conduct]. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL [and deputy/deputies] will undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

12. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety.
This policy will be reviewed every year by the Lead Co-Ordinator of E-Learning. At every review, the policy will be shared with the governing board.

13. Links with Other Policies

This Online Safety Policy is linked to our:

- Child Protection and Safeguarding Policy.
- Behaviour Policy.
- Staff Disciplinary Procedures.
- Data Protection Policy and Privacy Notices.

- Staff Acceptable Use Policy.
- Complaints Procedure.
- ICT and Internet Acceptable Use Policy.

Appendix 1: Acceptable Use Agreement (Pupils and Parents/Carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil:

- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the academy systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the academy systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.
- I will act as I expect others to act toward me.

(Pupil Acceptable Use Agreement continued)

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the academy:

- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the academy, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

Continued /

When using the internet for research or recreation, I recognise that: • I should ensure that I have permission to use the original work of others in my own work. • Where work is protected by copyright, I will not try to download copies (including music and videos). • When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me. **I understand that I am responsible for my actions, both in and out of school:** • I understand that the academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information). • I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.
Please note: If you do not sign and give consent, access will not be granted to school systems and devices.

Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS
Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material).
- Use them in any way which could harm the school's reputation.
- Access social networking sites or chat rooms.
- Use any improper language when communicating online, including in emails or other messaging services.
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network.
- Share my password with others or log in to the school's network/systems using someone else's details.
- Take photographs of pupils without checking the Digital Consent List.
- Share confidential information about the school, its pupils or staff, or other members of the community.
- Access, modify or share data I'm not authorised to access, modify or share.
- Promote private businesses, unless that business is directly related to the school.

I will :

- Lock my device when leaving it unattended.
- Report any data breaches or lost devices immediately. If a laptop, paper documents or other Trust / academy device is stolen, the member of staff should email help@hollingworthacademy.co.uk as soon as they are aware. If this happens in the evening or over a weekend, staff should email as soon as possible and not wait until they are next in school.
- I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
- I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's Data Protection Policy.
- I will let the Designated Safeguarding Lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where

these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/Academy/LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school/academy policy to disclose such information to an appropriate authority.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: Online Safety Training Needs – Self Audit for Staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's Acceptable Use Agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	