Online Safety Policy

Updated: September 2024

Approved by Trustees 18 September 2024

Review Date: September 2025

Contents

---

1. Aims

Our school aims to:

> Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors

> Identify and support groups of pupils that are potentially at greater risk of harm online than others

> Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')

> Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

> **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

> **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

> **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

> **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) 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 education and health 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.

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 make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

> Ensure 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 3)
> Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
> Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

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 designated safeguarding lead (DSL) 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 and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly

> Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks

> Working with the ICT manager to make sure the appropriate systems and processes are in place

> Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents

> Managing all online safety issues and incidents in line with the school's child protection policy

> Ensuring that any online safety incidents are logged (see appendix 5) 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 (appendix 4 contains a self-audit for staff on online safety training needs)

> 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

> Undertaking annual risk assessments that consider and reflect the risks children face

> Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

> Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept 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 monthly basis

> Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

> Ensuring that any online safety incidents are logged (see appendix 5) 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.

3.5 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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)

- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing by reporting immediately to the DSL / Deputies who will action the S4S Service team to support and enhance filtering mechanisms.
- Following the correct procedures by having authorisation from the Headteacher if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers 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/carers 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 resource sheet – Childnet International

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 3).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not

> That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous

> The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

> How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

> How information and data is shared and used online

> What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

> How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

> 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

> How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents/carers about online safety

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

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

> What systems the school uses to filter and monitor online use

> What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers 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 1 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. Class teacher will discuss cyber-bullying with their tutor groups.

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 safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents/carers so 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

> Poses a risk to staff or pupils, and/or

> Is identified in the school rules as a banned item for which a search can be carried out, and/or

> Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

> Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / DSL

> Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it

> Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

> Cause harm, and/or

> Undermine the safe environment of the school or disrupt teaching, and/or

> Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher or other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

> They reasonably suspect that its continued existence is likely to cause harm to any person, and/or

> The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

> **Not** view the image

> Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

> The DfE's latest guidance on searching, screening and confiscation

- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our Child Protection and Safeguarding Policy

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/carers, 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 to 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements.

8. Pupils using mobile devices in school

Pupils may require mobile devices for journeys to and from school, they are not permitted to be used during the school day, within:

- Lessons
- Class group time
- Clubs before or after school, or any other activities organised by school

 All mobile devices will be switched off and collected on entry and returned back to pupils at the end of the school day. Mobile devices collected will be locked in the school office during the school day. Devices are to be switched back on when pupils have left the premises

Any breach of the acceptable use of mobile devices by a pupil may trigger disciplinary action in line with the school behaviour policy and Child Protection and Safeguarding 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 8 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 by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use.

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 S4S Service team

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, Anti Bullying, Child Protection and Safeguarding and Acceptable ICT and internet Use Policy. 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 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 that 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).

By way of this training, all staff will be made aware that:

> Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

> Children can abuse their peers online through:

- o Abusive, harassing, and misogynistic messages

- o Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

- o Sharing of abusive images and pornography, to those who don't want to receive such content

> Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse

- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks

- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 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. An incident report log can be found in the appendix.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

> Child protection and safeguarding policy

> Behaviour policy

> Anti Bullying Policy

> Staff Code of Conduct

> Staff disciplinary procedures

> Data protection policy and privacy notices
> Complaints procedure
> ICT and internet acceptable use policy

Communications Technology
Staff, Volunteer, Student
Acceptable Use Policy

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to support management and learning without creating unnecessary risk to users while supporting learning.

I agree that I will:

- only use personal data securely
- implement the schools Computing and E-Safety policies
- educate pupils in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- educate pupils in the recognition of bias, unreliability and validity of sources
- actively educate learners to respect copyright law
- only use approved e-mail accounts in school
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified
- only give access to appropriate users when working with blogs or wikis etc...
- set strong passwords – a strong password is one which uses a combination of letters, numbers and other permitted signs
- report unsuitable content or activities to the E-Safety Leader/DSL
- ensure that videoconferencing is supervised appropriately for the learner's age
- read and sign the Acceptable Use Policy
- pass on any examples of Internet misuse to a senior member of staff
- post any supplied E-Safety guidance appropriately
- think carefully about what is stored on my laptop and make efforts to store sensitive data on the school server or private area on the Learning Platform

I agree that I will not visit Internet sites or make, post, download, upload or pass on: material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- promote private businesses
- breach any Local Authority/School policies, e.g. gambling
- do anything which exposes children to danger

- any other information which may be offensive to colleagues
- forward chain letters
- breach copyright law
- or access social networking sites or chat rooms
- Install any unauthorised software

I will not use any type of storage device / computing hardware that is used for storing, porting or extracting data files, information and objects or connect unauthorised hardware or devices to the school's network

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Name ………………………………………………..

Date ………………………………

Signed ….………………………………………………….

![Elston Hall Learning Trust logo]

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to support management and learning without creating unnecessary risk to users while supporting learning.

(1) Management Role:

As a Governor, I will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-safety leader and a named governor takes responsibility for e-safety
- an e-safety policy has been written by the school, building on Wolverhampton's LA e-safety (Digital Safeguarding) example and relevant guidance
- the e-safety and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is understood and not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URLs and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology (using the Self-Review Framework) to establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

(2) Accessing and/or Using School/Local Authority IT Systems and Facilities

As a Governor, I agree that I will:

- only use personal data/sensitive personal data securely
- adhere to the school's e-safety policy
- only use secure e-mail accounts when dealing with school personal data/sensitive personal data
- set strong passwords (using a combination of letters, numbers and other permitted signs)
- not reveal my password to anyone
- inform the Headteacher immediately if I believe someone else may have discovered my password
- report any security concerns to the Headteacher as soon as possible
- observe security guidelines at all times
- only store school personal data/sensitive personal data on the school server or private area on the school's learning platform, not on my personal computer/laptop/portable device
- not attempt to access any of the school's/LA's facilities using anyone else's login details

- not introduce or attempt to introduce any form of malicious software onto the school's/LA's management information system or learning platform
- not change or attempt to change or remove any part of the school's management information system or learning platform
- not deliberately delete files from the school's management information system or learning platform
- not edit, alter or use on any other website or social network site, any downloaded images or video obtained from the school's site.

I agree that I will not visit Internet sites or make, post, download, upload or pass on: material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- promote private businesses
- breach any Local Authority/School policies, e.g. gambling
- do anything which exposes children to danger
- any other information which may be offensive to colleagues
- forward chain letters
- breach copyright law
- or access social networking sites or chat rooms
- Install any unauthorised software

I will not use any type of storage device / computing hardware that is used for storing, porting or extracting data files, information and objects or connect unauthorised hardware or devices to the school's network

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

I agree to the terms and conditions above.

Name: …………………….………………………………………………

Signature: …………………………………………………………….

Date: ………………………………………………………………

ELSTON HALL
Learning Trust

Responsible Technology Use Agreement

When using technology in school:

- I will only access technology with the login and password that I have been given
- I will not access other people's files unless they are my Computing partner
- I will not bring in memory sticks from home to use on the network

When using the internet:

- I will ask permission before I access it
- I will report any material that makes me feel uncomfortable **immediately** to my teacher
- I understand that the school may check my files and monitor the sites that I visit
- I will not knowingly access social networking sites or chat rooms
- I will **never** give my full name, address, telephone number or agree to meet anyone
- I will not use search engines to find inappropriate material

I understand that:

- Using technology safely can make everyone's learning more enjoyable

General Internet Safety Tips for Home

- Always ask a grown up before you use the internet. They can help you find the best thing to do.
- Do not tell strangers where you live, your phone number or where you go to school. Only your friends and family need to know that.
- Do not send pictures to people you do not know. You don't want strangers looking at photos of you, your friends or your family.
- Tell a grown-up if you feel scared or unhappy about anything. Ask a grown up to help you put the Hector's World Safety Button on your computer/laptop/tablet. This will mean that you can press it if anything makes you scared or unhappy.
- You can also call 'Childline' on 0800 1111 to talk to someone who can help
- Did you know that Facebook, Instagram, Snapchat, TikTok and other social networking sites require you to be at least 13 years old to have an account
- WhatsApp requires you to be 16 years old to have an account.
    www.thinkuknow.co.uk   www.ceop.police.uk

www.elstonhallmat.co.uk

Guide to the Use of Images Online

Using Images Safely and Responsibly

We all enjoy and treasure images of our family and friends; family events, holidays and events are moments we all like to capture in photos or on video. All of which can be added to social network sites to be shared with family and friends.

However, we all have a responsibility to ensure we protect and safeguard all children and staff, including those who do not want to have their images stored online.

What are the risks of posting images online?

- Once posted and shared online any image or video can be copied and will stay online forever.
- Some children are at risk and **MUST NOT** have their image put online. Not all members of the community will know who they are.
- Some people do not want their images online for personal or religious reasons.
- Some children and staff may have a complex family background which means that sharing their image online can have unforeseen circumstances.

Therefore, at Elston Hall we are happy for parents and carers to take photos and video events for personal use but insist that these images are not distributed or put online in any way. This is to protect all members of the school community.

We thank you for your support,

Further Information on the Use of Images and Video:

Get Safe Online: https://www.getsafeonline.org/

Think U Know: https://www.thinkuknow.co.uk/parents/

Our website: https://www.elstonhallmat.co.uk/

Online safety incident report log

ONLINE SAFETY INCIDENT LOG					
Date	Where the incident took place	Description of the incident	Action taken	Review of filtering and monitoring and outcomes	Name and signature of staff member recording the incident

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?	
Are you aware of the ways pupils can abuse their peers online?	
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/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
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?	