The GALLERY TRUST

A community of special schools

Online Safety Policy
September 2023

The policy will be reviewed and updated following any updates to national and local guidance and procedures

Date ratified:	September 2023
Date for review:	September 2026
Chair of Trustees	Chris Scrivener
Chair of LAB	Matthew Willis
Designated Manager for Gallery Trust	Alison Beasley
Designated Trustee for Safeguarding	James Shryane

Contents:

Introduction

- Aims
- Our Approach
- Legislation and guidance

Roles and responsibilities

- The Headteacher
- The Designated Safeguarding Lead:
- Digital Technology Lead:
- All Staff and volunteers:
- Working with parents and carers:
- Visitors and members of the community

Educating Pupils about online safety

Preventing and addressing cyber-bullying

Examining electronic devices

Remote learning

Acceptable use of the internet in school

Pupils using mobile devices in school

Staff using personal devices in school

Staff using work devices outside school

Monitoring arrangements

Links with other policies

Appendix 1: Template EYFS and KS1 acceptable use agreement (pupils…

Appendix 2: Template KS2, KS3 and KS4 acceptable use agreement…

Appendix 3: acceptable use agreement (staff, governors, volunteers…

Appendix 4: Online Safety Staff Questionnaire

Introduction

Computing and the use of digital devices is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to provide our young people with the skills to access life-long learning and employment.

Computing and ICT covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of technology and computing within our society as a whole.

Whilst exciting and beneficial all users need to be aware of the range of risks associated with the use of these technologies.

At The Gallery Trust (The Trust) we understand the responsibility to educate our pupils on online safety; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies.

At The Trust we also recognise our responsibility to provide a safe environment for our students and that this includes ensuring appropriate filtering and monitoring systems are in place across our schools.

Both this policy and the Acceptable Use Agreement -for all staff, governors, visitors and pupils (see Appendix C) are inclusive of fixed and mobile internet technologies provided by the Trust and/or school. Any visitors using their own devices within school sign on entry to say that they adhere to the Trust's Acceptable Use Agreement and this online safety policy.

All staff, Trustees and LAB Members annual sign to confirm they have read and understood the content and their responsibilities in the latest Keeping Children Safe in Education, and other relevant safeguarding documents including the Child Protection and Safeguarding policy.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, board members, and Trust staff
- 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

Our Approach

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.
Commerce	Risks such as online gambling, inappropriate advertising, phishing and/or financial scams

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 and sex education
- Searching, screening and confiscation
- Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK

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.

This policy complies with our funding agreement and articles of association.

Roles and responsibilities

As online safety is an important aspect of strategic leadership within the school, the Trust, Head and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

Within each setting within the Trust, the DSL has overall responsibility for online safety; they can be supported by appropriately trained deputies and should liaise with other staff as appropriate, but this responsibility cannot be delegated. The Trust Safeguarding Manager (TSM) is responsible for quality assuring Safeguarding in the school, including the effective implementation of this policy.

Please refer to the school's Child Protection and Safeguarding Policy for the names of those holding key responsibilities in each school.

The Headteacher

The headteacher is responsible for ensuring:

- All staff are aware of this policy, and that it is being implemented consistently through the school
- The DSL is carrying out regular review of the online filtering and monitoring systems
- The curriculum includes online safety which is delivered at an appropriate level for all students.
- Job descriptions for DSL's include a statement around their responsibility for having the oversight for the monitoring and filtering of online systems

The Designated Safeguarding Lead:

Details of the school's DSL 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
- 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 which includes:
    - Raising awareness in recognising the signs and symptoms of online abuse
    - Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
    - The importance of reporting concerns around online use, including the monitoring and filtering of online devices
    - Children can abuse their peers online through:
        - Abusive, harassing, and misogynistic messages
        - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
        - 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
- Ensuring that new staff will receive training around online safety as part of their induction
- 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.
- Work with relevant leadership and teaching staff to ensure all students are taught how to keep themselves and others safe, including keeping safe online.
- Managing all online safety issues and incidents in line with the school child protection policy.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Oversight and management of the monitoring and filtering of the online system
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyberbullying 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 Local Academy Board.
- Carrying out termly reports with the Digital Technology Lead on the online monitoring and filtering systems
- Undertaking annual risk assessments that consider and reflect the risks children face
- Ensure that any lease or hire agreement refers to the responsibility of the organisation around online filtering and monitoring systems, and the statutory duty to report any concerns to the DSL and the Headteacher

This list is not intended to be exhaustive.

Digital Technology Lead:

The DTL 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 at a monthly basis.
- Carrying out termly reports with the DSL on the online monitoring and filtering systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on our behaviour recording system 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.

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 and ensuring that where appropriate pupils follow the school's terms on acceptable use Appendix 1: Template EYFS and KS1 acceptable use agreement (pupils… or Appendix 2: Template KS2, KS3 and KS4 acceptable use agreement…
- 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
- Contact the DSL and the DTM 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 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 and reported to the DSL
- 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

Working with parents and carers:

Parents/carers are requested to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure, if appropriate, 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)
- Notify their child's teacher or the DSL for the school if they have concerns about online safety at the school or their own child's online use including.

- Accessing inappropriate sites
- Sending inappropriate messages

The school will raise parents' awareness of internet safety through:

- Our website
- In letters
- Other communications with parents and carers
- This policy will also be made available to parents and carers through our website
- Information being shared and discussed at parents' evenings and other events

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.

Any organisations hiring or leasing our school building will need to provide reassurances around their understand of filtering and monitoring online devices and will be expected to report any concerns to the DSL or headteacher.

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 resource sheet – Childnet International

Educating Pupils about online safety

Pupils will be taught about online safety as part of the curriculum. Further details can be found within the school's curriculum documentation on request from the school.

Preventing and addressing cyber-bullying

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.)

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. School staff will discuss cyber-bullying with their classes/tutor groups.

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 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.

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 a criminal 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/appropriate staff member.
- 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 cooperation

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 a criminal offence

Staff will not actively seek to view the images, but there may be situations where the staff member needs to view the image to deem the seriousness of the image, or a student may show an image to a staff member before they are even aware of what the image is. Staff and students will be supported appropriately.

If inappropriate material is found on the device the staff member must inform the DSL or head teacher who will 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, the DSL/ headteacher/other member of the DSL team 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, the DSL/headteacher/other member of the DSL team 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 refuses to delete the material themselves, however the parent/carer will always be encouraged to delete the material from their child's device to ensure that they are taking the actions to protect their child

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** intentionally 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
- Immediately report to the DSL/headteacher/other member of the DSL team

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 behaviour policy / searches and confiscation 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.

Remote learning

The school's IT Support Provider will ensure that any device issued to staff / students for remote (home) learning have appropriate filtering and monitoring solutions in place before devices go off-site.

Devices and platforms issued by the school for teaching and learning will only be accessible to students via user-specific login credentials.

Parents will be notified, where appropriate, if an alert occurs whilst the device is in the home which raises concerns, and the device may be collected if this is felt appropriate. Parents are also given advice to contact the school if they have any concerns that their child is able to access any inappropriate content.

Devices are formatted to remove user data before reissue unless the user / device is subject to a policy infringement investigation.

The remote monitoring of student activities (with or without student consent) will only be carried out by a named, authorised person under the direction of the DSL.

Acceptable use of the internet in school

All pupils (where appropriate), parents, staff, volunteers, LAB members, Trust staff and Trustees are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet.

Appendix 1: Template EYFS and KS1 acceptable use agreement (pupils…

Appendix 2: Template KS2, KS3 and KS4 acceptable use agreement…

Appendix 3: acceptable use agreement (staff, governors, volunteers…

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 to 3.

Pupils using mobile devices in school

See the school behaviour policy for full details

Staff using personal devices in school

Staff will not use their personal devices during the school day unless, in exceptional circumstances, it has been agreed with the headteacher.

Staff should ensure that they provide family members/their own children's school/doctors etc with the school number as a contact number.

In exceptional circumstances the head teacher may approve arrangements around the staff member being able to answer the call during the school day.

Staff can refer to the staff code of conduct for full details.

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 which would violate the school's terms of acceptable use.

All staff sign an Acceptable Use Agreement to ensure they understand the expectations around acceptable use of school devices.

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 DSL or DTL.

Monitoring arrangements

The Trust's DSM will be monitoring the implementation of this policy across the Trust.

This policy will be reviewed every year by the DSM for The Gallery Trust. The review will be in accordance with KCSIE Keeping children safe in education - GOV.UK , and any other national and local guidance.

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
- Complaints procedure
- ICT and internet acceptable use policy
- Staff code of conduct

Appendix 1: Template EYFS and KS1 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:	
When I use the school's ICT systems (like computers) and get onto the internet in school I will: · Ask a teacher or adult if I can do so before using them · Only use websites that a teacher or adult has told me or allowed me to use · Tell my teacher immediately if: o I click on a website by mistake o I receive messages from people I don't know o I find anything that may upset or harm me or my friends · Use school computers for school work only · Be kind to others and not upset or be rude to them · Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly · Only use the username and password I have been given · Try my hardest to remember my username and password · Never share my password with anyone, including my friends · Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer · Save my work on the school network · Check with my teacher before I print anything · Log off or shut down a computer when I have finished using it **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer 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 will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: Template KS2, KS3 and KS4 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 read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

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 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, BOARD MEMBER, VOLUNTEERS AND VISITORS	
Name of staff member/board member/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 using someone else's details · Take photographs of pupils without checking with teachers first · 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 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.	
Signed (staff member/board member/volunteer/visitor):	Date:

Appendix 4: Online Safety Staff Questionnaire

ONLINE SAFETY TRAINING NEEDS QUESTIONNAIRE	
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?	
What ways are you aware of that pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Have you signed the school's acceptable use agreement for staff, volunteers, governors and visitors? Do you understand the expectations around this on you?	
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?	