Vision statement
BRIDGE is a family of schools committed to high performance. We embrace a universal culture of excellence in the learning communities we build.
Aims
To continue building a Multi Academy Trust that promotes strong values, an excellent education for all children, develops highly effective School Teams, is financially secure, and ensures effective governance.
To nurture, support and encourage aspirations by providing excellent learning opportunities, inspiring teaching environments, and a creative approach to curriculum subjects that secures engagement from all our learners resulting in high levels of academic progress and outcomes.
To develop outstanding leadership, teaching and support teams by valuing committed, reflective staff, and providing rigorous and challenging professional development for continual School Improvement.
To develop hubs as centres of learning excellence to disseminate best practice, firstly within and then beyond, the MAT.
To successfully engage and communicate with parents/carers in our local communities, supporting pupil progress, well-being and achievement.

Online Safety Policy

Purpose
To provide safe use of online technologies for staff, children and visitors

Spring 2021

Version	1.1	Next Review Date	Spring 2023

Contents

1. Aims

Bridge Schools Trust aims to:

- Have robust processes in place to ensure the online safety of children, 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

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

• content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

• contact: being subjected to harmful online interaction with other users; for example: 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; for example, 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. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Online safety is a running and interrelated theme whilst we devise and implement policies and procedures. We consider how online safety is reflected as required in all relevant policies and consider online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead and any parental engagement.

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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.

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

3. Roles and responsibilities

3.1 The Trustees

The Audit Committee will monitor Safegaurding arrangements and outcomes across the Trust. This will take place via the following mechanisms:

- Reports presented to the Board of Trustees by the Trust Safeguarding Lead

- Safeguarding Trustee monitoring of actions by the Trust Safeguarding Lead
- Trust feedback from LGB reports noting online safety and challenging as appropriate

3.2 The Trust Safeguarding Lead (TSL)- including Online safety

The Trust Safeguarding Lead will ensure that the Trust complies with all safeguarding requirements by:

- Monitoring online safety in all schools
- Ensuring that all school have appropriate training
- Supporting DSLs/Headteachers/Head of School to improve outcomes
- Supporting staff when dealing with incidents this may be to investigate, support with actions, sanctions or LADO involvement
- Liaise with technical staff to ensure robust filtering and reporting is effective
- Liaise with HR staff to ensure that policy and procedure is followed, taking appropriate action as necessary
- Attend up to date training and cascade where needed
- Provide training for Governors and Trustees as required

3.3 The Local Governing Body

The governing board has responsibility for monitoring safeguarding outcomes in the school, reviewing the effectiveness of this policy. The role of the Online Safety Governor (Safegaurding Governor) is to:

- Regularly meet with the DSL
- Monitor filtering reports and incident overviews provided by the school
- Feedback to Trustees via termly reports
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.4 The Headteacher/Head of School

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

- Ensuring the safety (including online safety) of members of the school community
- Being aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse", SWGfL)
- Ensuring that relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- Ensuring that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. Use SWGfL 360 review and S157 to support this.
- Sharing the monitoring and filtering overviews with the LGB

3.5 The School Designated Safeguarding Lead (Online Safety Lead)

Across Bridge Schools Trust, our Online Safety is embedded into the role of the Designated Safeguarding Lead, therefore these roles below, detail the focus on online safety within safeguarding our children.

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, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on My Concern and dealt with appropriately in line with this policy and the Trust Safeguarding Policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the Trust policies
- 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/Head of School and/or LGB/Trust Safeguarding Lead

This list is not intended to be exhaustive.

3.6 The IT Manager

Bridge Schools Trust has a managed IT service provided by outside contractors (mainly SOS Consultancy). These contractors receive regular safeguarding training and follow Trust policy and procedure. It is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school technical staff, as suggested below (in liaison with the Trust IT Manager).

The Trust IT Manager is responsible for leading schools and the outside contractors to:

- Put in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep children safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material (mainly through SWGfL)
- Ensure that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conduct a full security check and monitoring the school's IT systems regularly
- Block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Monitor use of the Trust Helpdesk system and revise as appropriate
- Liaise with the Trust GDPR Lead when disposing of IT goods, to follow the most recent guidance

This list is not intended to be exhaustive.

3.7 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 and following the Trust Code of Conduct

- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged on My Concern 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.

3.8 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Headteacher/Head of School 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 IT systems and internet (appendix 1), inline with the School's Home/School Agreement signed each Autumn Term.

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: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.9 Visitors and members of the community

Visitors and members of the community who use the school's IT 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 children about online safety

Children will be taught about online safety as part of the curriculum.

In **Key Stage 1**, children 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

Children 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

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

The school will use assemblies to raise childrens' awareness of the dangers that can be encountered online and may also invite speakers to talk to children about this; including the NSPCC.

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. This policy will also be available to parents.

Online safety will also be addressed during occasional parent sessions.

If parents have any queries or concerns in relation to online safety, these should be raised with any member of staff.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher/Head of School.

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 behaviour policy and safeguarding policy).

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that children understand what it is and what to do if they become aware of it happening to them or others. We will ensure that children 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 children, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Staff will discuss cyber-bullying with their children, and the issue will be addressed in assemblies.

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.

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 children, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL, alongside the Trust Safeguarding Lead 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.

7 Peer on Peer abuse

Everyone should be aware that children can abuse other children (often referred to as peer on peer abuse) and that it can happen both inside and outside of school and online. It is important that all staff recognise the indicators and signs of peer on peer abuse and know how to identify it and respond to reports. Peer on peer abuse is most likely to include bullying and online elements of which facilitates, threatening and/or encourages physical or emotional abuse. (please see Peer on Peer abuse policy for further detail)

Even if there are no reports in their schools it does not mean it is not happening, it may be the case that it is just not being reported.

8 Examining electronic devices including the use of mobile and smart technology

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 children's 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 children will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

9. Acceptable use of the internet in school

All children, parents, staff, volunteers, governors and visitors are expected to agree to the acceptable use of the school's IT systems and the internet (appendices 1 and 2). Children, parents and staff sign to say that they agree to this via the Home/School Agreement or the Staff Code of Conduct.

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 children, 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 and 2.

Where available, parents/carers and visitors will be given 'guest wifi', rather than staff access; if needed.

10. Children using mobile devices and smart technology in school

Children may bring mobile devices into school and leave them at the school office, but are not permitted to use them during the school day. This is mainly for those children who walk to/from school on their own.

11 Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

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

The acceptable use statements also refer to remote access, which is securely in place via agreed providers.

The school filtering system is not operated at the Central offices due to no children being on site.

12. How the school will respond to issues of misuse

Where a child misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour 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 disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The Trust will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

13. Remote Learning

Where children are being asked to learn online at home, we will follow the latest guidance from the Department to do so safely. We will also seek advice from the NSPCC and PSHE Association. See school website pages referring to remote learning for further information.

14. 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 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.

All staff should be aware that mental health problems can, in some cases, be an indicator that a child has suffered or is at risk of suffering abuse, neglect or exploitation.

More information about safeguarding training is set out in our child protection and safeguarding policy.

15. Cybercrime

We aim to prevent Cybercrime from happening across our trust. Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include;

• unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded;

• denial of Service (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and,

• making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime. If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests. Note that Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.

16. Monitoring arrangements

All staff log behaviour and safeguarding issues related to online safety. School DSLs monitor safeguarding procedures.

Safeguarding audits are conducted at least bi-annually, by the Trust Safeguarding Lead; this incudes online safety.

The Head of School/Headteacher must check online usage and can use the SWGfL report for this. This report must be taken to Local Governing Bodies at least annually. (see document on portal for further guidance)

Anti virus checks are overseen by the Trust IT manager via use of the helpdesk.

This policy will be reviewed at least every 3 years by the Trust Safeguarding Lead and IT Manager.

17. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Peer on Peer Abuse policy
- Behaviour policy and Anti-bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Staff Code of Conduct
- Home/School agreement

Appendix 1: acceptable use agreement (children and parents/carers)

To be displayed in classrooms and school entrances

Acceptable use of the school's IT systems and internet: agreement for children and parents/carers

All children at Bridge Schools Trust:

When using the school's IT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Access other children's work (unless my teacher has allowed me to)
- 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
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- 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/smart technology device into school:

- This will be kept at the office during school hours as it is for using if needed when walking to/from school. I will not use it during lessons, clubs or other activities organised by the school, without a teacher's permission
- School is not responsible for damage or loss to the phone/device. I am.
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language/intent when communicating online

I agree that the school will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's IT systems and internet responsibly.

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

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

To be displayed in school entrances and staff rooms

Acceptable use of the school's IT systems and the internet: agreement for staff, governors, volunteers and visitors

All staff members/governors/Trustees & Members/volunteers/visitors at Bridge Schools Trust:

When using the school's IT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal, pornographic or sexual nature
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language or attempt to harm/harass anyone when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school's network using someone else's details
- Use a memory stick on a work device (unless it has been encrypted)

I will only use the school's IT 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.

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 change my passwords regularly.

I will let the designated safeguarding lead (DSL) and IT manager know if a child 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 IT systems and internet responsibly, and ensure that pupils in my care do so too.

I will never contact school children directly using social media and will follow agreed advice from my Headteacher if another format is to be used ie email.

I will sign the staff code of conduct (or Governors code of conduct if appropriate) and ensure that all children/parents have signed the home/school agreement.

All images of children used on websites/social network/newsletters used outside of the physical school building, must not have any detail of the child's name. This is to deter people in the public domain from gaining information that may encourage innappropriate relationships with our children. Image use only.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.