THE BRIDGE
Alternative Provision

Online Safety Policy

Policy Reference	IT001
Author	IT Manager
Policy Agreed (date):	August 2024
Next Review (date):	August 2025
Approved by:	Executive Headteacher

Contents

Version Control

Version	Author	Date	Changes
V1.0	Executive Headteacher	April 2024	Review
V1.1	HR Director	August 2024	Updated to reformat and include version control and reference number.

1. Aims

Our provision aims to:

- Have robust processes in place to ensure the online safety of learners, staff and volunteers
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole provision 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 provisions on:

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

It also refers to the DfE's guidance on protecting children from radicalisation.

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

3. Roles and responsibilities

The Executive Headteacher

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

The designated safeguarding lead

Details of the provision's designated safeguarding lead (DSL) and 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 provision, in particular:

- Supporting the Executive Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the provision
- Working with the Executive Headteacher, IT 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 provision 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 provision 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 provision to the Executive Headteacher
- Implementing a digital safeguarding report tool to all learner devices.

This list is not intended to be exhaustive.

The IT manager

The IT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure learners are kept safe from potentially harmful and inappropriate content and contact online while at provision, including terrorist and extremist material.

- Ensuring that the provision'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 provision's ICT systems on a termly 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. The IT Manager needs to work closely with the DSL of each site to ensure it is logged appropriately and they follow the correct guidance.

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the provision 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 provision's ICT systems and the internet (appendix 3), and ensuring that learners follow the provision's terms on acceptable use (appendices 1 and 2)

- 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 provision 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.

Parents

Parents are expected to:

- Notify a member of staff or the Executive 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 provision's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre

- Hot topics – Childnet International

- Parent resource sheet – Childnet International

Visitors and members of the community

Visitors and members of the community who use the provision'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 learners about online safety

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

All provisions have to teach:

- Relationships education and health education in primary provisions

- Relationships and sex education and health education in secondary provisions

In Key Stage 3, learners will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy

- Recognise inappropriate content, contact and conduct, and know how to report concerns

Learners in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity

- How to report a range of concerns

By the end of secondary provision, learners will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online

- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- 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 learners with SEND.

5. Educating parents about online safety

The provision will raise parents' awareness of internet safety in letters or other communications home, and in information via our website under the category ADVICE HUB.

This policy will be shared with parents and online safety will also be covered during parents' evenings.

The provision will let parents know:

- What systems the provision 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 provision (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Executive Headteacher and/or the DSL.

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

6. Cyber-bullying

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 behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that learners understand what it is and what to do if they become aware of it happening to them or others. We will ensure that learners know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The provision will actively discuss cyber-bullying with learners , explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors 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 and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support learners , as part of safeguarding training (see section 11 for more detail).

The provision 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 provision will follow the processes set out in the provision behaviour policy. Where illegal, inappropriate or harmful material has been spread among learners , the provision 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 Executive Executive Headteacher, and any member of staff authorised to do so by the Executive Executive Headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or learners , and/or

- Is identified in the provision 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 learners and staff. If the search is not urgent, they will seek advice from the Executive Headteacher or DSL.
- Explain why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the device users 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 provision or disrupt teaching, and/or
- Commit an offence

If inappropriate material is suspected on the device, it is up to the Executive Headteacher and SLT 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 learner and/or the parent 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 learners 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 learners' electronic devices will be dealt with through the provision complaints procedure.

7. Acceptable use of the internet in the provision

All learners, parents, staff, volunteers (if appropriate) are expected to sign an agreement regarding the acceptable use of the provision's ICT systems and the internet (Appendices I to III). Visitors will be expected to read and agree to the provision's terms on acceptable use if relevant.

Use of the provision'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 learners , staff, volunteers and visitors (where relevant) to ensure they comply with the above using device monitoring and management software provided by Senso.

More information is set out in the acceptable use agreements in Appendices I to III.

8. Learners using mobile devices in the provision

Learners must hand their mobile phones to staff before entering the provision and these are then safely secured for the duration of the day. Phones are then handed back to learners as they leave the premises.

9. Staff using work devices outside the provision

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 provision's terms of acceptable use, as set out in Appendix III.

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 Executive Headteacher or Executive Business Manager.

10. How the provision will respond to issues of misuse

Where a learner misuses the provision's ICT systems or internet, we will follow the procedures set out in our policies. 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 provision's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training

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

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

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:
    - 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

Training will also help staff:

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

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

- Develop the ability to influence learners 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.

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 Appendix V. Monitoring and filtering logs are recorded on the Senso Administration Portal.

This policy will be reviewed every year by the Executive Headteacher.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy

- Behaviour policy

- Staff disciplinary procedures

- Data protection policy and privacy notices

- Complaints procedure

- ICT and internet acceptable use policy

Appendix 1 - EYFS & KS1 acceptable use agreement (learners and parents/carers)

ACCEPTABLE USE OF THE PROVISION'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR LEARNERS AND PARENTS/CARERS

Name of learner:	

When I use the provision's ICT systems (like computers) and get onto the internet in provision 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:
  - I click on a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use provision computers for provision work only
- Be kind to others and not upset or be rude to them
- Look after the provision 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 provision 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 provision will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (learner):	
Date:	

Parent/carer agreement:

I agree that my child can use the provision's ICT systems and internet when appropriately supervised by a member of provision staff. I agree to the conditions set out above for learners using the provision's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):	
Date:	

Appendix II - KS2, KS3 & KS4 acceptable use agreement (learners and parents/carers)

ACCEPTABLE USE OF THE PROVISION'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR LEARNERS AND PARENTS/CARERS

Name of learner:

I will read and follow the rules in the acceptable use agreement policy. When I use the provision's ICT systems (like computers) and get onto the internet in provision I will:

- Always use the provision'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 provision'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 provision:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the provision, 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 provision will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (learner):

Date:

Parent/carer agreement:

I agree that my child can use the provision's ICT systems and internet when appropriately supervised by a member of provision staff. I agree to the conditions set out above for learners using the provision's ICT systems and internet, and for using personal electronic devices in provision, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix III - Acceptable use agreement (staff, volunteers & visitors)

ACCEPTABLE USE OF THE PROVISION'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, VISITORS & VISITORS

Name of staff member/volunteer/visitor:	

When using the provision's ICT systems and accessing the internet in provision, or outside provision 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 provision'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 provision's network
- Share my password with others or log in to the provision's network using someone else's details
- Take photographs of learners without checking with teachers first
- Share confidential information about the provision, its learners 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 provision

I will only use the provision's ICT systems and access the internet in provision, or outside provision on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the provision will monitor the websites I visit and my use of the provision'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 provision, and keep all data securely stored in accordance with this policy and the provision's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a learner 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 provision's ICT systems and internet responsibly, and ensure that learners in my care do so too.

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

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 provision?	
Are you aware of the ways learners can abuse their peers online?	
Do you know what you must do if a learner approaches you with a concern or issue?	
Are you familiar with the provision's acceptable use agreement for staff, volunteers and visitors?	
Are you familiar with the provision's acceptable use agreement for learners and parents?	
Do you regularly change your password for accessing the provision's ICT systems?	
Are you familiar with the provision's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix V - Online safety incident report log

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