Bridgelea Pupil Referral Unit
Bridgelea Road
Withington
Manchester
M20 3FB

E-Safety and ICT Acceptable Use Policy

Implemented	**February 2021**
Presented by	**Rebecca Squires**
Review Date	**February 2024**

Bridgelea Primary School Vision & Mission Statement

Vision "Understanding People"

Mission Statement

"We work with people to build aspirations, connect, challenge, change and grow. We are an outstanding school and a proud founding member of the City of Manchester Learning Partnership."

- We value **SUCCESS**. Children achieve academic as well as social and emotional growth.
- We value **SAFETY**. We care for each other and keep each other safe.
- We value **CO-OPERATION**. As a school we will endeavour to co-operate with the community to inspire and empower every individual.
- We value **COMMUNICATION**. We believe that all behaviour is communication.
- We value **DEVELOPMENT**. Learning is understood developmentally.
- We value **WELLBEING**. We have a holistic approach to wellbeing across the school.
- We value **DIVERSITY**. We celebrate each other as unique individuals with rights that we respect.

UN Rights of the Child: Bridgelea 10 Articles

Through the School Council the children decided they would like to focus on the following 10 Articles, whilst understanding no right is more important than another:

Article 12
You have the right to give your opinion, and for adults to listen and take it seriously.
Article 13
You have the right to find out things and share what you think with others, by talking, drawing, writing or in any other way unless it harms or offends other people.
Article 15
You have the right to choose your own friends and join or set up groups, as long as it isn't harmful to others.
Article 24
You have the right to the best health care possible, safe water to drink, nutritious food, a clean and safe environment, and information to help you stay well.
Article 27
You have the right to food, clothing, a safe place to live and to have your basic needs met. You should not be disadvantaged so that you can't do many of the things other kids can do.
Article 28
You have the right to a good quality education. You should be encouraged to go to school to the highest level you can.
Article 29
Your education should help you use and develop your talents and abilities. It should also help you learn to live peacefully, protect the environment and respect other people.
Article 30
You have the right to practice your own culture, language and religion - or any you choose. Minority and indigenous groups need special protection of this right.
Article 31
You have the right to play and rest.
Article 39
You have the right to help if you've been hurt, neglected or badly treated.

The Six Principles Of Nurture

The nurturing approach offers a range of opportunities for children and young people to engage with missing early nurturing experiences, giving them the social and emotional skills to do well at school and with peers, develop their resilience and their capacity to deal more confidently with the trials and tribulations of life, for life.

1. Children's learning is understood developmentally
2. The classroom offers a safe base
3. The importance of nurture for the development of wellbeing
4. Language is a vital means of communication
5. All behaviour is communication
6. The importance of transition in children's lives

Rationale

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safety is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil and student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Un-authorised access to/loss or and sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with other, including strangers
- Cyber bullying
- Access to unsuitable video/internet games
- The potential for excessive use which my impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the offline world and it is essential that this e-safety policy be used in conjunction with other policies.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential through good educational provision to build pupils' resilience to the risks to which they may be exposed to and that they have the confidence and skills to face and deal with these risks.

Development

Role	**Named person**
ICT lead	Emma Spencer
Designated Safeguarding lead	Lisa Shaw
PHSE/Behaviour and attitude	Rebecca Squires

The Scope of the Policy

This policy applies to all members of Bridgelea Primary School (including staff, learners, volunteers, parents/carers, community users, visitors) who have access to and are users of ICT systems, both in and outside of Bridgelea.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of Bridgelea.

The 2011 Education Act increased these powers with regard to the search for and of electronic devices and the deletion of data. In the case of both of these acts action can only be taken in relation to our current behaviour policy.

This policy is to be read in conjunction with the Acceptable use of ICT Policy, Relationships Policy, Safeguarding Policy, PHSE guidance, RSE Policy and Anti-bullying Policy.

The school will deal with such incidents within the policy and associated behaviour and anti-bullying policies and will, where known, inform parents/ carers of inappropriate e-safety behaviour that takes place out of school.

Roles and responsibilities.

Governors-

Governors are responsible for the approval of the E safety policy and for reviewing its effectiveness.

Headteacher and Senior Leadership Team

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community- though the day-to-day responsibility of e-safety will be delegated to the DSL and Behaviour and Attitudes Lead of SLT.
- The Headteacher is responsible for the implementation and effectiveness of this policy. He is responsible for reporting to the Governing Body on the effectiveness of the policy, and, if necessary, make any necessary recommendations of further improvement
- The headteacher/senior leaders are responsible for ensuring that the ICT lead/DSL have adequate training to take out their roles.
- The headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of these in school who carry out the internal e-safety monitoring role.
- If there is an allegation against a member of staff, the Headteacher should be aware of the procedures to follow.

ICT Lead/DSL/AHT

- Take day to day responsibility for e-safety and the responsibility for documents and policies
- Ensure staff are aware of all procedures
- Report any breaches of policy to SLT
- Provide training and advice to staff
- Liaise with the LA where necessary
- Log all reports of e-safety issues on CPOMs
- Are trained in and have shared with staff and awareness and understanding of e-safety issues and the potential for serious child protection issues that can arise from

Sharing of Personal Data

Access to illegal/inappropriate material

Inappropriate online contact with adults/strangers

Potential or actual incidents of grooming

Cyber-bullying

Sexting

Revenge pornography

Radicalisation (Extreme views)

CSE

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that-

- They have an up-to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read understood and signed the E-Safety policy and the Acceptable use of ICT policy and adhere to the guidance around communications detailed in the Acceptable use of ICT policy.
- They report any suspected issue or problem to the ICT lead/DSL for investigation/action/sanction
- Pupils understand and follow the school policies.
- Pupils should be aware of how to deal with unsuitable material as detailed in the RSE and ICT curriculum

Pupils

- Pupils are responsible for using ICT systems in accordance with policy. This is included in the admissions process of Bridgelea
- They need to understand the importance of reporting abuse/misuse or access to inappropriate materials and know how to do so.
- Should understand that E-safety extends to out of school.

Parents/Carer

Parents and carers have a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research suggests that many parents/carers do not fully understand the issues and are less experienced in the use of ICT than their children are. The school will therefore take every opportunity to help parent s to understand these issues through-

- Parent/carer workshops
- Letters and newsletters
- Drop in meetings with SLT if necessary around E-safety concerns
- Website

Parents and carers should be aware that school has a responsibility to safeguard pupils. The misuse of non-school provided systems outside of school hours will not be investigated by the school. It remains the responsibility of parents and carers to ensure that they are adequately supervising their child and are positively promoting E-safety awareness within the home. Failure to do this could result in a safeguarding issue, which may need to reported to Children's Social Care or Greater Manchester Police.

Parents are advised to monitor all online activities of their children using one of the following apps-

- Ourpact
- Go Bubble.

Curriculum coverage-

E-Safety is taught as part of a spiral curriculum, which permeates the curriculum offer. Discrete teaching takes place around E-Safety under RSE education and computing lessons. This is further enhanced by the use of assemblies, theme weeks and pastoral activities as part of our nurturing curriculum. Where there are specific concerns, intervention may be offered via our retreat team.

Milepost	Coverage in ICT	Coverage in RSE	Additional Theme weeks and foci. (All mileposts)
1	Recognise common uses of technology beyond school. 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 • Keeping usernames and passwords private • Know the implications of inappropriate online searches	How can I keep safe online? What are the rules for keeping safe at school and outside school?	**Anti Bullying week (Autumn 2)** **Safer Internet Day (Spring 1)** **Mental Health Awareness week (Summer 1)** RRS assemblies.

2	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 • Know the importance of secure passwords • Know a range of ways of reporting inappropriate contact.	What are the ways of communicating online? (data sharing) What does it does it mean to have responsibility over my actions (online vs offline behaviour/online privacy) (Also- work around good quality sleep is covered here)	
3	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 • Identify more discrete inappropriate behaviours • Have a secure knowledge of common online safety rules.	How can the internet positive and negatively affect our mental health? Why is it important to be critical of the media? How do I stay safe on a mobile or a tablet?	

Why is ICT systems access important?

Technology offers unimaginable opportunities and is constantly evolving. Access is currently becoming universal and increasingly more mobile, and learners are using technology at an even earlier age. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

ICT systems at Bridgelea increase the opportunities for learners to access a wide range of resources in support of the curriculum and learning. It supports the professional work of staff and enhances the school's management information and business administration practice.

Access to Bridgelea's network and the internet is necessary for staff and learners. It is an entitlement for all learners as it helps them to develop a responsible and mature approach to accessing information.

How will internet access within school be authorised?

- Internet access is a necessary part of the statutory curriculum. It is an entitlement for learners based on responsible use
- Parents will be informed during the admissions meeting that learners will be provided with monitored internet access
- Parents will be asked to sign and return the consent form

How will the risks be assessed?

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for learners. Bridgelea will supervise learners and take all reasonable precautions to limit users access and that users access only appropriate material. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that unsuitable material will never appear on a terminal. If this does happen it should be reported to a member of the SLT immediately.

- The use of computer systems without permission or for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990
- Methods to identify, assess and minimise risks will be reviewed regularly
- Staff, parents, governors and advisers will work to establish agreement that every reasonable measure is being taken
- The Head Teacher will ensure that the policy is implemented effectively.

How will Bridgelea ensure internet/ICT access is safe for pupils and staff? (Infrastructure/equipment).

- All users will be informed via this policy that Internet use will be monitored
- School ICT systems will be managed through the managed service provider in ways that ensure that the schools meets the e-safety technical requirements for Manchester Council. This is provided by One Education.
- One Education are the schools internet and ICT provider who are responsible for monitoring our Web filtering alongside the DSL, using Sophos web filtering systems.
- Any failure of the filtering systems will be reported directly to the ICT technical team via admin staff at each site
- Bridgelea will work in partnership with parents, the statutory authorities, the DFE and the Internet Service Provider to ensure systems to protect learners are reviewed and improved where necessary

- If staff or learners discover unsuitable sites, the URL (address) and content will be reported to the ICT technical team via admin staff at each site
- Any material that Bridgelea suspects is illegal will be referred to the appropriate authorities
- Servers, wireless systems and cabling must be securely located and physical access restricted (server room).
- All users will have clearly defined access rights to school ICT systems.
- Staff will be made responsible for their username and password, must not allow other users to access the systems using their log on details, and must immediately report any suspicion or evidence that there has been a breach.
- Remote management tools are used by the managed service provider to control workstations and view user's activity and there is additional protection against viruses.
- Appropriate service measures are in place provided by the service provider to protect the servers, firewalls, routers, wireless systems etc. from accidental or malicious attempts that might threaten the security of the schools systems and data.
- Personal data is sent via Egress secure and all personal information is handled in compliance with the GDPR policy

How will e-mail be managed?

- Communications with persons and organisations will be managed to ensure appropriate educational use and that the good name of Bridgelea is maintained
- Any digital communication between staff and parents/ carers must be professional in tone and content and be via official school email
- Users need to aware the email communications may be monitored
- Users must immediately report to the SLT, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email

How will publishing on the Web be managed?

- The Headteacher will delegate editorial responsibility to a members of the SLT to ensure that content is accurate and quality of presentation is maintained
- The point of contact on the website will be the school admin email address and telephone number. Home information or individual e-mail identities will not be published
- Photographs published on the Web will not have full names attached and anonymity will be protected where necessary as stipulated in admissions paperwork and permissions.
- The above rules apply for publication on the school Twitter handle, which is managed by a member of SLT.

The use of digital photographs and video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood for potential for harm:

- Staff are allowed to take digital/ video images to support educational aims but must follow school policies concerning the storing, sharing distribution and publication of these images. These images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes

- Care should be taken when taking digital/ video images that pupils are appropriately dressed and they are not participating in activities that might bring individuals or the school into disrepute
- Pupils must not take, share, use, publish or distribute images of others without their permission
- Photographs published on the website or elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images
- Pupils full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents/ carers will be obtained before photographs of pupils are published on the school website or newsletter
- Staff should refer to the Staff Handbook and code of conduct for guidance around social media and pupils.

How will staff and learners be informed of the policy?

- All staff will be provided with the E- safety and ICT Acceptable Use policy, and its importance will be explained. The policy will be made available to parents on request.
- E-Safety will be a key focus in all areas of the curriculum and staff will reinforce e- safety messages across the curriculum through assemblies and nurture breakfast and lunchtimes.

Monitoring

The Headteacher and SLT will monitor the impact of the policy using:

- Pupils, parent/ carer, governor and staff feedback
- Iris and CPOMs logs of reported incidents
- Internet monitoring by class teams on a regular basis

Appendices

1. Responsible Internet Use Statement for pupils, staff and visitors and guidance for students on cyberbullying

2. Rules for pupils to be displayed in classrooms and next to all computers

3. Letters to parents on Responsible Internet Use

4. Consent Form

Appendix 1

Responsible Internet Use
Rules for Staff, Visitors and pupils

- The computer system is owned by the school. This Responsible Internet Use Statement helps to protect pupils, staff and the school by clearly stating what use of the computer resources is acceptable and what is not

- Irresponsible use may result in the loss of internet access and could lead to disciplinary proceedings for staff

- Network access must be made via the user's authorized account and password, which must not be given to any other person

- School computer internet use must be appropriate to the pupils development and curriculum content or to the staff professional activity

- The use of chat rooms is not permitted

- Copyright and intellectual property must be respected

- Email should be written carefully and politely, particularly as messages may be forwarded or printed and be seen by unexpected readers

- Users are responsible for emails sent and contacts made

- The ICT systems may only be used for private purposes during staff break time and in designated spaces.

- The school my exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of email and the deletion of inappropriate materials where it believes unauthorized use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorized or unlawful text, imagery or sound.

Cyberbullying guidance for pupils

If you believe you or someone else is the victim of cyberbullying you must speak to an adult as soon as possible.

- Do not answer abusive messages and report them to an adult
- Do not delete anything until it has been shown to an adult (even if it is upsetting)
- Do not give out any of your personal IT details
- Do not reply to abusive emails
- Never reply to someone you do not know

Appendix 2

Bridgelea Pupil Referral Unit
Rules for responsible computer and internet use

The school has installed computers and internet access to help your learning. These rules will keep everyone safe and help us to be fair to others.

- I will not log in as another person or access other people's files

- I will not bring in USBs or CD ROMs from outside school unless I have been given permission
- I will use the internet only when a member of staff is present
- I will only use the printer with permission
- I will not enter chat rooms
- I will only email people I know or a member of staff has approved
- My messages will be polite and responsible
- I will not give out my home address or telephone number or arrange to meet anyone
- I will report any message or websites that make me feel uncomfortable

- I understand that school may check my computer files and may monitor the internet sites I visit

Appendix 3

Dear parents/ carers

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, Bridgelea Pupil Referral Unit is providing supervised access to the internet. We believe that the effective use of the World Wide Web and email is worthwhile and is an essential skill for children as they grow up in the modern world.

Please read the attached Rules for Responsible Internet Use and sign and return the consent form so that your child may use the internet at school.

We have provided you with a copy of the 'E-Safety and Acceptable Use Policy '. If you wish to discuss this with a member of staff please contact school.

Although there are concerns about students potentially having access to undesirable materials, we have taken positive steps to reduce this risk in school. Bridgelea Pupil Referral Unit operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavor is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, and pupils will not be left unsupervised, the school cannot be held responsible for the nature or content of materials accessed through the Internet.

Please support us by ensuring that internet usage at home is supervised and reinforce the rules of appropriate and safe use.

Yours sincerely

Phil Hoyland

Headteacher

Appendix 4

Consent Form

Bridgelea Pupil Referral Unit
Responsible Internet Use

Please complete, sign and return to the office

Pupil name:	

Pupil's Agreement

I have read and I understand the school Rules for Responsible Computer Use. I will use the computer system and Internet in a responsible way and follow these rules at all times.

Signed:	

Parent's Consent for Internet Access

I have read and understood the school rules for responsible Internet use and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials.

I will monitor my sons/daughters internet usage at home.

Signed:	***Date:***

Please print name: