**Bridgelea Pupil Referral Unit**
**Bridgelea Road**
**Withington**
**Manchester**
**M20 3FB**

# E-Safety and ICT Acceptable Use Policy

| Implemented | September 2017 |
|---|---|
| Presented by | Nichala Johansen |
| Review Date | September 2018 |

**The Scope of the Policy**

This policy applies to all members of Bridgelea PRU (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 PRU.

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 PRU.

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 ICT Policy, Behaviour Policy, Safeguarding 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.

**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 PRU 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 PRU'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 PRU 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 PRU ensure internet access is safe for pupils and staff?**

- All users will be informed via this policy that Internet use will be monitored
- Any failure of the filtering systems will be reported directly to the ICT technical team via admin staff at each site
- Bridgelea PRU reserves the right to remove access to any website it considers inappropriate
- Bridgelea PRU 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 PRU suspects is illegal will be referred to the appropriate authorities
- All staff at Bridgelea PRU are made aware of e-safety issues and receive annual up-to-date training from the DSL and Personal Development, Behaviour and Welfare Lead
- All learners will receive training and guidance on the use of personal devices via the curriculum, assemblies and nurture class time
- All learners receive a planned and developmentally appropriate e-safety curriculum that teaches them how to stay safe, protect themselves from harm and how to take responsibility for their own and others safety.
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and learning activities
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where learners are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- Reporting routes are clearly understood by all staff at Bridgelea, for example online anonymous reporting systems (CEOP Report Abuse button).

**Parents/Carers E Learning Support**

Parents/Carers play a crucial role in ensuring that their child understands the need to use the internet in an appropriate way. Bridgelea PRU will take every opportunity to help parents understand these issues through website information and e-safety literature. Parents and Carers will be encouraged to support Bridgelea PRU in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents sections of the website

**How will the security of the school ICT system be maintained?**

- The whole system will be reviewed with regard to threats or potential threats from external internet access
- No personal data should be sent over the internet unless it is encrypted or otherwise secured
- Virus protection will be installed and updated regularly
- Devices that are taken and used away from the school will be subject to regular scrutiny to ensure that malicious applications do not breach network security systems and that no data is inappropriately removed from the site.

**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 PRU 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
- A group email address will be provided to all classes for Smart School Council use
- Individual email addresses may be provided to some KS2 pupils if deemed appropriate. Alongside this they will taught about the strategies to deal with inappropriate emails and reminded of the need to write emails clearly and correctly
- 

**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

**The use of Social Media**

- Social media sites such as Facebook and Twitter cannot be used for learning purposes.
- Staff should not authorise friend or follow requests from learners.

**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

## Cyberbullying

Learners are taught about the proper use of telecommunications and about the serious consequences of cyber bullying. Bridgelea will through PHSE and in ICT lessons and assemblies, continue to educate and inform and educate learners about these fast changing areas of ICT technology

- Staff will undertake annual training on cyberbullying
- Incidents will be logged on Iris and CPOS, the schools behaviour and safeguarding recording systems

## Guidance for Staff who suspect Cyberbullying

If you suspect or are told about a cyberbullying incident, follow the protocol outlined below:

- Ask to see the mobile phone/ computer and note clearly everything that is on the screen, including date, time and names.
- Ask the pupil to save the message/ image
- If a parent is reporting an incident, ask them to do the same and send a copy to the school admin email address.
- Report the incident to a member of SLT and record on CPOMS

## How will incidents be handled?

The management of the acceptable use of the Internet in school is achieved by:

- Protection software installed on the network;
- Acceptable Use Policy adopted by the school;
- Staff handbook containing this policy signed for by the appropriate staff;
- A range of disciplinary procedures for infringements of the policy

It is more likely that the school will have to deal with inappropriate rather than illegal misuse. It is important that incidents are dealt with as soon as possible and in a proportionate manner.

Whenever a learner or staff member infringes the policy, the final decision on the level of sanction will be at the discretion of the Headteacher and/ or Governors.

The following activities will be considered a breach of Bridgelea PRU code of staff conduct and will result in disciplinary action.

- Excessive use of Internet for personal activities not related to professional development
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1998
- Bringing the school name into disrepute
- Befriending learners on personal social media accounts

## 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

# 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 endeavour 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**<br>**Responsible Internet Use**<br><br>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:*** | |