Bright Horizons

Burnley Brow
Community School

Safeguarding: e-Safety and ICT Acceptable Use Policy For Staff and Children

Burnley Brow Community School

Reviewed December 2012
Reviewed/ Ratified/ Shared with Staff October 2013
Ratified/ Shared with Staff December 2014/2015
Updated and shared Feb 2017
Updated and shared Feb 2018

e-Safety and Acceptable Usage

At Burnley Brow we are committed to the use of ICT to enhance and enrich teaching and learning opportunities and experiences for all learners.

This policy sets out clearly our expectations of pupils, staff, parents and visitors to ensure best practice. This policy has been written with reference to Oldham Local Safeguarding Children Board, e-Safety Policy and Guidance notes. Whilst this document constitutes a full e-Safety policy reference to e-Safety and this policy must be reflected in our school policies on:

- Safeguarding
- Child Protection
- Anti-Bullying
- Curriculum

Burnley Brow e-Safety Lead and Child Protection Lead

At Burnley Brow the overall responsibility for Child Protection and e-Safety lies with the Headteacher, however, a team of designated staff lead on this. The Headteacher reports to the Governors on a termly basis.

Safeguarding is a serious matter; at Burnley Brow we use technology and the internet extensively across all areas of the curriculum and ensure that it is comprehensive, age-related and effective. Online safeguarding, known as e-Safety is an area that is constantly evolving and at Burnley Brow we ensure that staff CPD is current and included in staff induction; as such this policy will be reviewed on an annual basis or in response to an e-Safety incident, whichever is sooner.

Pupils' Access to the Internet and Network Safety:

All users log on to the network using a username and password. On the network there are "public drive" areas where many different groups of users can save work so that it is available to others. Pupils are taught how to access and save to these shared resource areas. Teachers use the "teacher drive" to share files with each other; children do not have access to these files.
All users of the network can be monitored remotely by the network administrators and all users are aware of this.

Internet Safety:

When using networked equipment all access to the Internet is protected by a number of different filters. These filters are designed to prevent accidental or deliberate access to unsuitable materials. In addition, the network administrators can manually block site addresses which are considered to be unacceptable. However, no system is 100% safe and pupils are taught that the Internet contains many websites that are useful but that there are also websites that are unpleasant, offensive or which introduce software which can damage the equipment. No-one must attempt to access a website that they know to be unsuitable for children and/or containing offensive language, images, games or other media. At Burnley Brow, we have an e-Safety curriculum which is integrated into our Computing curriculum, which has been designed to teach the children how to keep themselves safe whilst using the internet. We also cover this issue annually during our Anti-Bullying themed week/ days. We also regularly have an additional Computing and E-safety Themed Weeks, Themed Days or Performances.

The Head Teacher/ICT Lead will ensure these procedures are followed by staff in the event of any misuse of the internet:

An inappropriate website is accessed inadvertently:

- Report website address to the ICT lead, who will then log the incident.
- Contact the filtering service so that the site can be added to the banned or restricted list.

An inappropriate website is accessed deliberately:

- Report website to the ICT lead, who will then log the incident.
- Contact the filtering service so that the site can be added to the banned or restricted list.
- Decide on appropriate action (if young person).

An adult receives inappropriate material:

- Do not forward this material to anyone else.
- Log website address, log off and alert the ICT lead immediately.
- Ensure the nature of the material is logged.
- Contact relevant authorities for further advice e.g. police, social care, CEOP.

An illegal website is accessed or illegal material or evidence of illegal activity is found on a computer:
This may contain racist, obscene or violent materials.

If any of the above are found, the following should occur:

- Alert the Headteacher/ICT lead immediately.
- DO NOT LOG OFF the computer and bring the computer to be kept in a safe place.
- Contact the police / CEOP and social care immediately.
- If a member of staff or volunteer is involved, refer to the Disciplinary Policy and report to the Local Authority Designated Officer.

Threatening or malicious comments are posted to the school's learning platform- DB Primary (or printed out), about an adult or child in school, or in the instance that malicious text messages are sent to another child/young person (cyber bullying):

- Preserve any evidence and log the incident.
- Inform the Headteacher immediately and follow Child Protection Policy.
- Inform the Child Protection Lead.
- Check the filter if an internet-based website issue.
- Contact/parents and carers.
- Contact the police or CEOP if appropriate.

Pupils accessing the Internet at home are subject to the controls placed upon them by their parents. To support parents in safeguarding their children, on the school website we publish specific advice for parents with regards eSafety and how best to protect their child in this respect. We also share this advice via newsletters on a regular basis, and hold annual parent classes on this issue. However, any home use of the Internet made in connection with the school or school activities; will be subject to this policy and any breach dealt with as if the event took place at school.

Prevent

Prevent is a safeguarding issue, protecting young people from being drawn into terrorism and ensuring action is taken when they observe behaviour of concern.

In relation to Prevent, the following Government definitions are used:

- **Terrorism** is an action that endangers or causes serious violence to a person/people; causes serious damage to property; or seriously interferes or disrupts an electronic system. The use or threat must be designed to influence the government or to intimidate the public and is made for the purpose of advancing a political, religious or ideological cause. (Terrorism Act, 2000)

- **Extremism** is vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs. It also includes calls for the death of members of the UK armed forces, whether in this country or overseas. (Prevent Strategy, 2011)

- **Fundamental British values** are defined as democracy, the rule of law, individual liberty, and mutual respect and tolerance of those with different faiths and beliefs. (Prevent Strategy, 2011)

- **Radicalisation** is the process by which a person comes to support terrorism and forms of extremism leading to terrorism.

Staff and Governors are aware of Prevent and have received Government training on this. Children are also made aware of Prevent through their Computing curriculum. The Prevent Duty lead in school, the Headteacher, should be notified of any concerns if staff feel an individual is being radicalised or is vulnerable to radicalisation into extremism.

Email Safety:

We do not allow pupils to send emails externally. Children only use email through the VLE (DB Primary) and can only communicate in this way to their class and their teachers. They are taught how to use DB Primary safely and how to communicate appropriately through email. Staff use the First Class e-mail system, and both should only be used for school purposes.

VLE (Virtual Learning Environment):

Burnley Brow uses a Virtual Learning Environment called DB Primary, which is a social online space for teachers and children to share learning both at home and in school. The site is completely secure and every child and teacher in school has an individual username and account. Children are taught to press the 'whistle' on their screens if they see something inappropriate. An email is automatically sent to the Deputy Head who will deal with the problem. The ICT subject leader and Deputy Head has the administration account log in details and can access any account at any time. All pupils sign an agreement at the beginning of each school year to show they are agreeing to follow the rules regarding e-Safety. Anyone not following the rules for DB Primary will have their accounts deactivated for a period of time. Children's internet activity can be monitored remotely and their parents are aware of this.

All children agree to the following before being allowed to use our VLE:

- *I will not tell anybody my password for DB Primary.*
- *I will tell my teacher if I think someone knows my password.*
- *I will blow the whistle on the screen if I see something inappropriate.*
- *I understand that the things I write on DB Primary are* ***public*** *and can be seen by all the teachers.*
- *I understand that I shouldn't share private information online.*
- *I will use DB Primary to complete homework assignments and for communicating in a sensible and appropriate way.*
- *I understand that if I do not follow these rules, my account will be disabled for an agreed time.*

We run parent classes to keep our parents informed about our VLE and to show them how to support their child with this at home.

Facebook and Social Networking:

Burnley Brow uses a Facebook business account to engage parents in the life of the school and celebrate learning achievements and notices with them. The page is monitored by the ICT lead. Staff do not engage with this page to protect their own online privacy.

Staff who make use of personal social networking accounts should not mention their place of work or anything work-related that could incriminate them. Members of staff should never add or accept pupils, ex-pupils or parents as friends. If a member of staff knows a member of one of these groups outside of school, then they should consult with the Headteacher before adding or accepting them. Many staff members use platforms such as Twitter for CPD purposes. We encourage staff to use social networking in this way, but only during non-contact time and staff should never share sensitive information or anything which could negatively affect the school's image. Staff are asked to state where necessary that views are their own and may not represent the views of the school.

The children at Burnley Brow are taught about the risks of social networking and are taught how to minimise those risks. We also provide parent classes on e-Safety and offer support and advice for parents to protect themselves and their family online.

Mobile Devices/Phones:

Pupils are not allowed mobile phones or personal electronic devices in school - any such items brought in must be handed to the office or kept by the class teacher and returned to parents at the end of the day.

Mobile devices belonging to staff should not be used to store children's personal data. No personal data such as home addresses, contact telephone numbers, medical information, photographs should be kept on such devices.

Digital Images:

Parents sign an annual consent form for the use of images of their children for school purposes and on the internet: the school website, social media etc - the child's full name is never included with their image. Digital images may be shared with partner schools and organisations as part of collaborative learning projects. All such use is monitored and supervised by staff.

Members of staff do not use their personal cameras/ mobile phones to photograph children. Equipment is provided by the school for such purposes.

E-Bullying:

The school takes bullying very seriously and has robust procedures for identifying and dealing with it. Pupils are taught about bullying as part of the curriculum. Bullying of any type will not be tolerated by the school and will be dealt with under the procedures within the Whole School Policy on Behaviour, Safety and Wellbeing Policy.

Acceptable Use Policy for Staff:
Staff ICT Agreements

Computers, laptops and other networked resources, including internet access, are available to staff in the school. It is expected that staff will use computers as appropriate within the curriculum and that they will provide guidance and instruction to pupils in the safe use of ICT.

Internet access is provided to staff to support work related activities. All users should be polite to others and use appropriate language.

- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.
- I have read the Procedures for Incidents of Misuse so that I can deal effectively with any problems that may arise.
- I will report accidental misuse.
- I will report any incidents of concern for children or young people's safety to the Headteacher, Designated Person/Team for Child Protection or ICT Lead.
- I will not communicate with pupils via e-mail, phone, social networking.
- I will ensure that I keep my password secure and do not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the ICT Lead.
- I will not allow pupils to use my laptop when I am logged on as staff.
- I am aware that my e-mails, internet use and files may be monitored, and by communicating in this way, I am aware that I am a representative of the school and must remain professional and adhere to policies and procedures in place at all times.
- I will adhere to copyright and intellectual property rights.
- I will not use school computers/devices for commercial purposes which could bring the school or yourself.
- I will ensure that if I open files from removable media such as: CDs, flashdrives and mobiles; they have been checked with antivirus software.
- I will ensure that I do not leave my laptop unattended in view e.g. in my car. Insurance policies may not cover this.
- I will report all faults to the technician who will prioritise work to be done.

By using the school network, internet and ICT equipment you are agreeing to abide by this policy. Any violation of these provisions will result in access to a laptop, the school network and the Internet being denied and may result in disciplinary action.