Safeguarding: Online Safety and ICT Acceptable Use Policy for Staff and Children

Reviewed December 2012, Reviewed/ Ratified/ Shared October 2013, Ratified December 2014, Updated2017,Feb 2018, May 2019/Sept 2021, November 2022, May 2023

Review Date: May 2024

Statement of Intent

Burnley Brow understands that the use of ICT and online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. Their use is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The governing body is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the Designated Safeguard Lead's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Headteacher is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedure, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the Designated Safeguarding Lead (DSL) and the deputy DSLs by ensuring they have sufficient time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date, and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of this.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.

The Designated Safeguarding Lead (DSL) is responsible for:

- Taking the lead responsibility for online safety in school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Understanding the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Ensuring that online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies as required.
- Working closely with the police during police investigations.
- Keeping up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in national online safety events.
- Dealing with online safety incidents and inappropriate internet use, both by pupils and staff.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in school's provision and using this data to update the school's procedures.
- Reporting to the governing body regarding online safety when needed.

All staff members are responsible for:

- Adhering to the Acceptable Use Agreement. (Appendix 1)
- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are responsible for:

- Following the Acceptable Use Agreement that they sign in September. (Appendix 2)
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures in this policy.

Managing Online Safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The importance of online safety is integrated throughout school in the following ways:

- Staff and governors receive regular training
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted on the topic of remaining safe online.

Handling Online Safety Concerns

Any disclosures made by pupils to staff members about online abuse, harassment, or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Safeguarding: Child Protection Policy.

Staff will be aware that pupils may not feel ready or know how to tell someone about the abuse they are experiencing, due to feeling embarrassed or threatened. Staff will make it clear to the child that confidentiality cannot be promised.

Any concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action. If the concern is about the headteacher, it is reported to the Chair of Governors. Concerns regarding a pupil's online behaviour are reported to the DSL.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

Cyberbullying

Cyberbullying can include, but is not limited to, the following

- Threatening, intimidating, or upsetting text messages.
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras.
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible.
- Threatening or bullying emails possibly sent using a pseudonym or someone else's name.
- Unpleasant messages sent via instant messaging.
- Unpleasant or defamatory information posted to logs, personal websites and social networking sites.
- Discriminatory bullying online.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Behaviour Policy.

Child-on-child Sexual Abuse and Harassment

Pupils may use the internet and technology as a vehicle for sexual abuse and harassment both, off and online. They will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating, or encouraging sexual violence
- Upskirting i.e. taking a picture of underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks

- Sexualised online bullying e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children e.g. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed and distributed with the permission of the child depicted, or by the child themselves.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse are reported to the DSL who will investigate the matter in line with the Safeguarding Child Protection Policy.

Grooming and Exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- The pupils may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming.

Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent e.g. sexual coercion and encouraging children to behave sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser. Whilst these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

When staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment e.g. individuals in extremist groups identifying, targeting and contact young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being radicalised. Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL.

Mental Health

The internet, particularly social media can be the root cause of a number of mental health issues in pupils. Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. Concerns about mental health of a pupil will be dealt with in line with the Emotional Health and Wellbeing Policy.

Online hoaxes and harmful online challenges

For the purpose of this policy, 'harmful online challenges' refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge and distributing it through online media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL. The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about where quick local action can prevent a hoax or challenge from spreading more widely.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed with the relevant pupils. The DSL and the Headteacher will only implement a school-wide approach to highlight the potential harms of a hoax or challenge.

Cyber-Crime

Cyber-crime is a criminal activity using computers and/or the internet.

Cyber-enabled: these crimes can be carried out offline, however, are made easier and can be conducted at higher scales and speeds online e.g. fraud.

Cyber-dependent: these crimes can only be carried out online or by using a computer e.g. making supplying or obtaining malware, illegal hacking etc.

The school will factor into its approach to online safety the risk that pupils with a particular affinity of skill in technology may become involved.

The DSL and Headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology on school-owned devices or on school networks through the use of firewalls.

Online Safety Training for Staff

All safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Online Safety and the Curriculum

Online safety is embedded throughout the curriculum; however it is particularly addressed in the Computing and PSHRE curriculum. Online safety teaching is always appropriate to pupils' ages and developmental stages. Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safety and confidently regardless of the device, platform or app they are using. Pupils with SEND and LAC children may need more support to stay safe online.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships look like
- Self-esteem
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate.

Class teachers must view any external resources prior to using them to ensure they are appropriate for the cohort of children they are teaching.

If a staff member is concerned about anything pupils raise during online safety lessons, they must let the DSL know immediately.

At Burnley Brow, we have an e-Safety curriculum, integrated into the Computing curriculum, which has been designed to teach the children how to keep themselves safe whilst using the internet. It is also covered annually during our Anti-Bullying themed week/days, computing and e-Safety themed weeks, themed days or performances.

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.

The Head Teacher/RANATECH 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 RANATECH, 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 RANATECH, 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.

An adult receives inappropriate material:

- Do not forward this material to anyone else.
- Log website address, log off and alert the Headteacher 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 immediately.
- DO NOT LOG OFF the device but do bring it 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, 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 Safeguarding 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 e-Safety 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.

Use of technology in the classroom
A range of technology is using during lessons including:

- Laptops
- Chromebooks
- iPads

Prior to using any website, tool, apps or other online platforms in the classroom or at home the teacher must review and evaluate the resource.

Educating Parents
The school works in partnership with parents to ensure pupils stay safe online at school and at home. Parent Workshops are held.

Emails
Access to and the use of emails is managed in line with the Data Protection Policy. Staff members are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Staff members must block any spam and junk mail and report the matter to RANATECH. Personal emails are not permitted to be used for any schoolwork. We do not allow pupils to send emails externally, they are encouraged to contact their class teacher if needed through Google Classroom.

Facebook and Social Networking
Burnley Brow uses a Twitter account to engage parents and the community in the life of the school and celebrate learning achievements and notices with them. The page is managed by the Headteacher. 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. To protect pupil safety, staff should not share the location of trips and visits. 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 the workplace, then they should consult with the Headteacher before adding or accepting them. Staff should ensure their account is private and should check that their profile images (including previous profile images) are appropriate. Staff should be mindful of their professional reputation before posting or sharing images or posts online. Staff should also consider using a variation of their name to increase their online privacy.

Staff should be aware that if an account is public, any member of a network can see posts shared. Tagging a location to a post can also make personal information vulnerable, therefore, staff are advised to prevent their social media platform from automatically adding locations to posts. Being tagged in a public post can increase the likelihood of staff profiles being viewed by a wide audience, therefore, staff are advised to check that security settings require any tags in photo or posts to be approved before they 'go live'. If staff members suspect that personal posts or photos have been accessed or shared by a pupil, they should consult the Headteacher. Staff are advised to screenshot any evidence and speak to the Headteacher as soon as possible so that the matter can be investigated. This will also prepare the Headteacher for any possible parental complaints. In this scenario, it is recommended that staff locate the original posts or photos and make them private or remove them from social media. Staff are advised to remove any photographs that could impact their professional reputation.

In order to check online reputation and test privacy settings, it is recommended that staff search their own name regularly on a search engine and then check the results and images. Any images or

information that could compromise a staff member's professional reputation should be captured in a screenshot and the matter should be taken to the Headteacher. Staff should not reply or comment on such posts but should instead use the reporting features of the host site. If staff members find an account set up in their name, but which does not belong to them, then they should again let the Headteacher know and contact the site involved in order to have the accounts removed.

Any staff members who use platforms such as Twitter for CPD purposes are encouraged 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. If using social media for professional purposes to showcase achievements and discuss issues affecting education, staff should ensure that their online username and profile picture is professional. Staff are asked to state where necessary that views are their own and may not represent the views of the school.

If a staff member becomes aware of inappropriate content on social media involving pupils, they should inform school as soon as possible by speaking to the Headteacher and then appropriate steps should be taken to ensure the child's safety. Certain issues like cyberbullying, self-harming or children putting themselves or others at risk should be referred as a safeguarding concern. Staff should take a screenshot of any inappropriate content relating to school, staff, or pupils in order to evidence any concerns.

School Website
The headteacher is responsible for the overall content of the school website. They will ensure that the content is appropriate, accurate, up-to-date and meets government requirements. Personal information relating to staff is not published on the website. Images and videos and only posted on the website if permission is given.

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 or photographs should be kept on such devices. Mobile phones and personal devices should not be used in teaching areas or any areas that the children might pass through.

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.

Remote Learning
The school will make sure that any school-owned equipment for remote learning will have suitable anti-virus installed and will liaise with parents during this period of Remote Learning. See the Remote Education Policy.

Appendix 1
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 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.
- I will not communicate with pupils via e-mail, phone or 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/ RANATECH.
- 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 into disrepute.
- I will ensure if I open files from removable media such as: CDs, flashdrives and mobiles; that they have first 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 RANATECH who will prioritise work to be done.

Every staff member/trainee/supply staff must sign that they have read and understand this policy agreement.

By using the school network, internet and ICT equipment you are demonstrating agreement 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.

This policy will be signed annually by existing school staff:
Phase leaders will ensure class teachers and TAs sign in the phase file.

Strategy will sign the policy and ensure admin and site staff also sign that copy.

DHT will ensure all trainees sign their copy.

Admin will add to induction to check it has been read and signed.
Admin will give a copy to supply staff to read and sign.

Appendix 2

Google Classroom Safety Rule and Expectations.

- Only put appropriate content on the stream.
- If you are unhappy about something that you have received from someone, or any content on the page, you must report it immediately.
- You can send messages to your teachers through Google Classroom. Remember, important issues are best discussed in person as your teacher may not see your message straight away.
- Do not spend too much time on Google Classroom at home, the internet can become addictive and affect your sleep and health.
- If you cannot access your tasks at home, please speak to your class teacher.
- Your teacher will use Google Classroom with you and set you tasks, and you are expected to complete them, just like you would with any other homework.

Please remember that the adults in school can see what you are accessing and the messages you are sending – any inappropriate language or content will be flagged to your teachers.