Bricknell Primary School

ONLINE SAFETY POLICY

Safeguarding Team	
Head of School	Hannah Stannard
Designated Safeguarding Lead	Nicola Waites
Deputy Safeguarding Lead	Fay Littleproud
Online Safety Lead	Nicola Waites
Designated Governor for Child Protection and Safeguarding	Tanya Freeman
Behaviour Lead	Matthew Mullen
SENCO	Vicki Jones

INTRODUCTION

Online Safety describes the use of new technologies involving mobile devices and the internet safely. Under this umbrella we aim to educate pupils about the benefits of using emerging technologies as a means of collaboration and production whilst maintaining an emphasis on awareness and evaluation of risks related to these new technologies.

The school's Online Safety Policy operates in conjunction with other school policies: Relationships and Behaviour Policy, Safeguarding and Child Protection Policy, Anti-bullying Policy, Data Protection and PSHE Policy.

Our Online Safety Policy is in accordance with Hull Safeguarding Children Partnership's Guidelines and Procedures which can be accessed via http://www.proceduresonline.com/hull/scb/

Online Safety teaching and maintenance can be seen across school at different levels:

- Responsible and secure use of ICT by all adults as an example to pupils.
- Clear and published policies regarding aspects of administration and curriculum.
- Monitoring reports generated by Esafe Global to highlight possible breaches or incidents.
- Safe and secure internet access provided by KC and filtered through Smoothwall with management from RM Education.

This policy applies to all aspects of the school, including out of hours provision e.g. clubs run by staff and outside providers.

LEARNING AND TEACHING

Members of the school community including students, staff, governors, parents and carers are educated on the benefits and risks of using new and emerging technologies in different ways. Safe and responsible behaviour when using these technologies is promoted throughout school by a number of means:

- Specific Online Safety lessons which follow the Project EVOLVE toolkit which is based on UKCIS framework "Education for a Connected World" (EFACW)
- Assemblies and whole-school activities such as Safer Internet Day.
- Reactive sessions and workshops when opportunities/risks arise.

- Use of age appropriate internet tools to support learning.
- Reminders of personal accountability through an end-user Acceptable Use Policy (AUP) which is displayed when logging on to a laptop.
- Clearly visible methods of reporting inappropriate content/behaviour for in and out of school.

STAFF TRAINING

Staff receive regular Online Safety training in the form of inset sessions and are updated to new and emerging risks where appropriate. Staff receive regular information bulletins from National Online Safety and complete an annual online safety course.
Staff are made aware of responsibilities regarding Online Safety and safeguarding pupils, whilst also maintaining awareness of reporting procedures.

ICT SYSTEMS

Bricknell Primary School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a computer. Neither Bricknell Primary School nor the Constellation Trust can accept liability for the material accessed, stored or distributed or any consequences resulting from Internet use.
Bricknell Primary School must audit digital technological use to establish if the e–safety policy is adequate and that the implementation of the e–safety policy is appropriate.
The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
Methods to identify, assess and minimise risks will be reviewed regularly.

Staff are responsible for ensuring that ICT systems are used safely and securely by themselves and pupils in their care. Devices and access to technologies are controlled and moderated by the Computing Subject Leader and RM Education. Antivirus and system tools are always kept up to date to ensure appropriate protection.

Access to technologies is controlled by school staff and varying levels of supervision and access are dispensed by RM Education, along with class teachers.

All users of school computers have an individual username and password which is kept secure. All users agree to an end-user Acceptable Use Policy (AUP) at the point of login to school devices. This policy acts as a reminder of the rules, regulations and guidelines to using school technology. Staff must ensure that workstations are locked when not using them to limit access to potentially confidential information and elevated access to school systems.

E-MAIL

Staff and pupils have an allocated email address provided by MSN and monitored by RM Education. Use of personal email accounts for transfer of school documentation is prohibited.

All email contact with parents, carers and other stakeholders is done through the use of official school email accounts or approved means such as Tapestry and it is encouraged that other

relevant staff are copied in where appropriate.

Pupils are reminded to report any inappropriate email content/behaviour using clearly visible reporting procedures.

PUBLISHING

Bricknell Primary School will control access to social media and social networking sites. Children will be advised never to give out personal details of any kind which may identify them and/or their location to persons unknown or through unsecured sites. Examples would include their real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

Children must be advised not to place personal photos or videos on any unsecured social network space. They must consider how public the information is and consider using private areas. Advice must be given regarding background detail (such as a school crest) in a photograph or video which could identify the child or his/her location.

Organisational blogs or social media sites must be password protected and run from the organisational website with approval from the Senior Leadership Team/Senior Manager. Employees/volunteers must be advised not to run social network spaces for children's use on a personal basis.

If personal publishing is to be used with children and young people then it must use age appropriate sites suitable for educational purposes and the site must be moderated by organisational staff. They must be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Children must be encouraged to invite known friends only and deny access to others by making profiles private.

Children are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Copyright must be held by the school or attributed to the owner where permission to reproduce has been obtained.

Permission from parents/guardians, in the form of an agreement signed on school enrolment, must be obtained before publishing photographs/video.

Official school accounts must be used to post all content. No personal accounts should be used for any reason.

In addition to these guidelines, staff are to ensure that any online presence they hold such as on social networks or blogs is in keeping with their professional standards. Staff members must not engage in any activity which would be damaging to the school such as posting inappropriate content or participating in online messaging about sensitive or damaging issues.

Staff must be aware of privacy settings on personal accounts and should ensure that reasonable safeguards are put in place to prevent pupils contacting these accounts. Staff who hold an account should not have pupils as 'friends' or contacts unless the account has been opened for the specific official use of school for home links and has been approved by school leadership.

FILTERING AND MONITORING

Intentional or accidental interaction with inappropriate or sensitive materials may be blocked through filters provided by Smoothwall and monitored by eSafe Global. These subjects and materials may include (but are not limited to) the following:

- Discrimination – Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, culture or sex
- Drugs/Substance abuse – displays or promotes the illegal use of drugs or substance
- Extremism – promotes terrorism and terrorist ideology, violence or intolerance
- Malware/Hacking – promotes the compromising system, including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
- Pornography – displays sexual acts or explicit images
- Piracy and copyright – includes illegal provision and copyright materials
- Self-harm – promotes or displays deliberate self- harm (including suicide & eating disorder)
- Violence – displays or promotes the use of physical force intended to hurt or harm.

FILTERING

Internet use is filtered through the use of a Smoothwall filter which is maintained and monitored by RM Education. Pupils and staff are reminded of their responsibilities regarding safe and secure use of technology and clear reporting procedures are in place using desktop shortcuts to report inappropriate content and also key members of staff being prominent and available to pupils as an alternative. Either method of reporting must reach the Online Safety Lead. The school will liaise with the relevant agencies such as RM Education, Smoothwall, E-Safe, the local authority or CEOP when responding to incidents.

Exceptions to the list of websites filtered can be made on the discretion of the Computing subject leader in conjunction with guidance from the Online Safety Lead and the Senior Leadership Team (SLT). Continuous evaluation of usefulness and appropriateness of digital content is a skill which is promoted and pupils are encouraged to play an active role in this.

MONITORING

Whilst directly accessing technology, children are monitored physically by their teacher and other members of staff present. This requires staff to be present and vigilant and reflects our school's current situation: few e-safeguarding incidents lead to a conclusion of low risk. This will be amended if circumstances change.

All internet traffic is logged within the Smoothwall Admin Console and is accessible to the Computing subject leader or RM Education on request. Staff and children enrolled at Bricknell

Primary School have their internet access and history logged within this system.

Incidents which involve violation of the filters (see above section: Filtering) are identified by the software, E-Safe, which the school uses to trigger a notification to both the Online Safety Lead and Head of School for action (see below section: Response to Incidents of Concern). The school uses software from ESafe Global to monitor internet use of all users on the school network, reporting breaches and incidents to the Online Safety Lead at appropriate intervals depending on the severity of case.

EMERGING TECHNOLOGIES

New and emerging technologies are regularly examined regarding their educational purpose and corresponding risk. New technologies are evaluated before being used in school.

Children are to be involved in the monitoring and evaluation of emerging technologies (including apps) through regular 'open floor' sessions involving the pupils and the Online Safety Lead.

MOBILE AND PERSONAL DEVICES

Pupils

While we acknowledge a parent's/carer's right to allow their child to bring a mobile phone to school, Bricknell Primary School discourages pupils from bringing mobile phones and electronic devices to school. In general, pupils should not bring valuable items to school as they can be lost or stolen. Parents are reminded that in cases of emergency, the school office remains a vital and appropriate point of contact.

Where parents allow children to bring a mobile phone or electronic device to school, they do so entirely at their own risk. The school accepts no responsibility for any loss or damage whilst it is on school premises. Only pupils in Year 6 are permitted to bring mobile phones into school and the parents of these pupils must have signed and returned a mobile phone protocol that they must have shared with their child. If a pupil brings a mobile phone to school, they must turn it off before entering the school site and this must be locked away inside their bag inside their locker. Any pupils failing to adhere to the mobile phone protocol will have their phones confiscated and they will need to be collected by a parent from a member of the SLT.

If a pupil is found taking photographs or video footage with any electronic device of either, other pupils or members of staff, this will be regarded as a serious matter and disciplinary action will be taken in accordance with the school's Relationship and Behaviour Policy.

Staff

It is fully recognised that imposing rigid regulations on the actions of others can be counterproductive. An agreement of trust is therefore promoted regarding the carrying and use of mobile phones and personal devices within our school setting, which is agreed to by all users.

- Staff are not permitted to use mobile phones or personal devices whilst carrying out

any duty that involves supervision or contact with children (with the exception of trips and visits where mobile phones may be used to facilitate the health and safety of the members of the party).
- Staff will not use their mobile phones or personal devices in pupils' presence unless prior permission has been obtained from the Head of School.
- Staff are not at any time permitted to use recording equipment on their mobile phones or personal devices, for example: to take photographs or videos of children, or share images and will only use work-provided equipment for this purpose.

As per EYFS statutory guidance, staff must not use electronic devices in rooms where children are present, including those where children are cared for.

It is appropriate to take photographs of children to capture a curriculum activity or a celebration of school life using school equipment, providing we have permission to do so from the parents.

Any pupil who accesses the internet, via a mobile phone network or smart technology (3G, 4G and 5G) to intimidate, threaten, commit an offence or cause harm to others whilst on the school site will not be tolerated. If appropriate, actions will be taken in accordance with the school's Relationship and Behaviour Policy and/or Child Protection and Safeguarding Policy, which may include referring the matter to the police and/or Children's Social Care.

Parents

While we would prefer parents not to use their mobile phones or electronic devices while at school, we recognise that this would be impossible to regulate and that many parents see their phones as an essential means of communication. We therefore ask that parents' usage of devices, whilst on the school site is courteous and appropriate to the school environment.
We ask that parents who take photographs or videos of school events, such as shows or sports day, ensure that it is for personal use and is not posted on any social media platforms. There may be occasions when, due to safeguarding issues, parents are asked not to take photographs or videos of such events.

SMARTWATCHES

Smartwatches and similar devices, which have their own means of cellular connectivity or internet access, are not permitted to be worn by staff or children.

INTERNET ACCESS

Bricknell Primary School will maintain a current record of all staff/volunteers, children and young people who are granted access to the organisation's electronic communication systems.
All staff/volunteers must read and sign the organisation's policies regarding information security and the use of information technology before using the organisation's ICT resource.

For Foundation stage children, access to the Internet will be by adult demonstration with occasional directly-supervised access to specific, approved on-line materials.

As with use of devices, access to the internet is controlled by school and varying levels of supervision and access are administered by RM Education.

SANCTIONS

Misuse of the internet may result in disciplinary action, including written warnings, withdrawal of access privileges, and in extreme cases, suspension or expulsion, in accordance with the school's Relationship and Behaviour Policy. The school also reserves the right to report any illegal activities to the appropriate authorities.

SCREEN, SEARCHING AND CONFISCATION

The Education Act 2011, allows staff to lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used in the following ways:

- to cause harm,
- to disrupt teaching,
- to break school rules,
- to commit an offence,
- to cause personal injury, or
- to damage property.

If it is alleged that a device contains sexual images of children, staff must not view the content and refer the matter immediately to the DSL, who will contact the police.

GENERAL DATA PROTECTION (GDPR) AND ONLINE SAFETY

Data must always be processed lawfully, fairly and transparently; collected for specific and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected.

GDPR is relevant to Online Safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.

Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the school population and external stakeholders, particularly, but not exclusively: pupils, parents, staff and external agencies.

Personal and sensitive information should only be sent by email when on a secure network.

Personal data should only be stored on secure devices.

In the event of a data breach, the school will notify the Data Protection Officer (DPO) immediately, who may need to inform the Information Commissioner's Office (ICO).

ASSETS

- Details of all school owned hardware will be recorded in a hardware inventory both in hardcopy and electronically.
- Details of all school owned software will be recorded in a software inventory both in hardcopy and electronically.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (amended) Regulations 2007. See Environmental Agency website for details.

PARENTAL SUPPORT

Parents' attention is drawn to the school Online Safety Policy and regular updates to content are maintained in different ways:

- Newsletters.
- School website.
- National Online Safety Updates
- Parent workshops.

Parents are kept involved with pupils' Online Safety education and must sign the agreement prior to pupils being granted internet access at school. Parents are also reminded of the AUP which all pupils adhere to.

RESPONSE TO AN INCIDENT OF CONCERN

Online sexual exploitation

Bricknell Primary School will be vigilant in relation to child sexual exploitation and online grooming. Staff/volunteers will be made aware of the organisation's protocols and responsibilities in relation to online grooming including how and with whom to share information and concerns.

Bricknell Primary School will record any issues and will report any concerns about a child's safety to Children's Social Care.

Bricknell Primary School will develop approaches to educate children, young people and parents on the dangers of online grooming and sexting.

Sex and Relationship Education and/or PHSE may be an opportunity to explore issues including consent, sexting, appropriate relationships, pornography use and protective steps children and young people can take online.

Sexting

Bricknell Primary School will make children aware of the risks associated with the creating, storing and sharing of images of a sexual nature. Clear procedure, adhering to the 'Response to Risk Flowchart' (below), is in place to support anyone affected by 'sexting'; including appropriate referrals to Children's Social Care and/or the Police and organisational responses including involvement of Child Protection Co-ordinators and Online Safety leads.

Online sexual harassment

Sexual harassment is likely to: violate a child's dignity, make them feel intimated, degraded or

humiliated and/or create a hostile, offensive or sexualised environment.
Online sexual harassment, which might include: non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats.
Any reports of online sexual harassment will be taken seriously, and the police and Children's Social Care may be notified.
Our school follows and adheres to the national guidance - UKCCIS: Sexting in schools and colleges: Responding to incidents and safeguarding young people, 2016.

Cyber-bullying

Cyber-bullying (along with all forms of bullying) will not be tolerated in Bricknell Primary School. Full details are set out in Bricknell Primary School's policy on anti-bullying. All incidents of cyberbullying reported to Bricknell Primary School will be recorded. Children and young people, staff and parents/carers will be advised to keep a record of the bullying as evidence. Bricknell Primary School will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

An important element of E-Safeguarding is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff/volunteers, children and young people have a responsibility to report online safety or e-security incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The school has incident reporting procedures in place and records incidents on CPOMs.

Response to Risk Flowchart

Response to and Reporting of an E-safety Incident of Concern