Online Safety Policy

Brindishe Schools

Document status	
Author	Alex Lea and Rebekah Chin
Creation	23.10.20
Version	2
Date of next review	October 2022
Approval Body	Federation Governing Body

Development/Monitoring/Review of this Policy

This online safety policy has been developed by a working group made up of:

- Senior Leaders
- Online Safety Coordinators
- IT managers
- Governors
- Parents and carers

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Federation Governing Body	*Awaiting approval*
The implementation of this online safety policy will be monitored by the:	*The online safety team for each school led by Alex Lea, Rebekah Chin and Ciara Cullen*
Monitoring will take place at regular intervals:	*Review to take place Summer 1*
The Federation Governing Body will receive a report on the implementation of the online safety policy generated by the online safety team (which will include anonymous details of online safety incidents) at regular intervals:	*Following the review in Summer 1*
The online safety policy will be reviewed annually, or more regularly in the light of significant developments in the use of technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*October 2021*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*School's designated safeguarding leads and the Federation Governing Body*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of
    - students
    - parents/carers
    - staff

Why an Online Safety Policy

The rapid growth of the internet and the availability of a wide range of digital/mobile technologies accessible to all is both exciting and challenging. Whilst benefiting from the learning and communication opportunities, the inherent issues and risks must be properly assessed. Children and adults need to be educated and supported to develop the necessary skills to keep themselves safe and develop digital resilience when using technology. This policy is to be read alongside our 'Child Protection and Safeguarding Policy', IT and Social Networking Protocol for staff, Data Protection and Fair Access Policy and our schools' Whistleblowing Policy.

With this policy we:

- Set out the key principles expected of all members of the school community at Brindishe schools with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Have clear structures to deal with online abuse such as online bullying, grooming, sexual images, sexual exploitation and radicalisation.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Ensure that all members of the school community are fully aware that inappropriate or unsafe behaviour is unacceptable and will be challenged and addressed through the necessary channels.
- Minimise the risk associated with inappropriate use of Internet and IT technology.

Scope of the Policy

- This policy applies to all members of the Brindishe Frederation community (including staff, children, volunteers, parents/carers, visitors, community users) who have access to and are users of the schools' digital technology systems, and digital technologies both in and out of the schools.
- The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of Children 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 online-bullying or other online safety incidents covered by this policy, which may take place outside of the schools, but is linked to membership of the Brindishe Federation.
- The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Online Safety Policy and with express permission from parent/carer.
- Brindishe Federation will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the Brindishe Federation.

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor alongside their existing role as the Child Protection and Safeguarding Governor.

The role of the Online Safety *Governor* will include:

- regular meetings with the Online Safety Co-ordinators
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors meeting

Headteachers and Executive Head

- The Headteachers have a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Leads.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. The Executive Head will be informed if an allegation is made against the Head Teacher.
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Leads.

Online Safety Lead

Brindishe Green – Rebekah Chin
Brindishe Manor – Ciara Cullen
Brindishe Lee - Alex Lea
These leads will:

- lead the Online Safety Group.
- take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the schools' online safety policies/documents.
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provide training and advice for staff.
- liaise with schools' IT managers.
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments.
- meet regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs.
- attend relevant meetings of Governors.
- reports regularly to Senior Leadership Team.

IT Managers

Those with technical responsibilities are responsible for ensuring:

- that the schools' technical infrastructures are secure and are not open to misuse or malicious attack.
- that users may only access the networks and devices through a properly enforced password protection policy.
- that they keep up-to-date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteachers, Senior Leaders and Online Safety Leads for investigation/action/sanction.
- that monitoring software/systems are implemented and updated as agreed in the Brindishe Schools policies.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current Brindishe Federation online safety policy and practices.
- they have read, understood and signed the staff Acceptable Use policy.
- they report any suspected misuse or problem to the Headteacher/Senior Leader for investigation/action/sanction. If the suspected misuse is by the Headteacher or Senior Leader they should report to the Executive Head.
- all digital communications with children/parents/carers should be on a professional level and only carried out using official school systems.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- children understand and follow the Online Safety Policy and Acceptable Use policies.

- children have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned, children 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.

Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

They should carry out their duties as outlined in the child protection and safeguarding policy.

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the *Schools'* community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives.

Members of the Online Safety Group will assist the Online Safety Leads with:

- the production/review/monitoring of the schools' online safety policy/documents.
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression.
- monitoring network/internet/filtering/incident logs.
- consulting stakeholders – including parents/carers and the Children about the online safety provision.
- monitoring improvement actions identified through use of the 360safe self-review tool.

Children

- are responsible for using the schools' digital technology systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras including on iPads and tablets. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that Schools' online safety policy covers their actions out of school, if related to their membership of the school.

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Brindishe Schools will take every opportunity to help parents understand these issues through parents' evenings, newsletter bulletins, letters, the website and information about national/local online safety campaigns/literature (For example, Safer Internet Day). Parents and carers will be encouraged to support the schools in promoting good online 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/Learning Platform Itslearning.
- their own and their children's personal devices in the schools.

Community Users who access school systems or programmes as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Educating our community

Brindishe schools will ensure children's safety, by providing a curriculum that is age-appropriate and supports children's learning across the curriculum, so that the wider school community has the necessary knowledge to take a responsible and resilient approach to the risks of using digital technologies/the internet.

Educating our children

Online Safety education will be provided in the following ways:

- Specific teaching will be provided as part of Computing, PHSME, RSE and other curriculum areas (as relevant) and should be regularly revisited – this will cover both safe use of IT and new technologies in school and outside school.
- Children should be helped to understand the need for the children's Acceptable Use agreement and encouraged to adopt safe and responsible use of both within and outside of school.
- Children will be given clear objectives for internet use and encouraged to learn what use is acceptable and what is not. Where children are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- Websites recommended as part of home learning will have been checked for appropriate content and in lessons where internet use is pre-planned, it is best practice that children 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.
- Students/pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making .
- Children should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Staff will model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright.

- The school will ensure that the use of materials from the Internet complies with copyright law.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Children will be shown how to publish and present information appropriately to a wider audience.
- Key online safety messages should be reinforced as part of a planned programme of assemblies (e.g. Safer Internet Day) and during day-to-day discussions and opportunities.

Vulnerable Learners

At Brindishe Schools we recognise that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.

When implementing an appropriate online safety policy and curriculum we will seek input from specialist staff as appropriate, including the Inclusion Leads.

Awareness and Educating parents / carers

Parents and carers have an essential role in the monitoring / regulation of the children's access to IT, online experiences and online safety risks at home and out of school.

The schools will support parents/ carers to minimize any risks associated with inappropriate use of internet and / or IT technology. We will do this through:

- Guidance and support through signposting online safety activities
- Newsletters/ Letters
- Parent/carer/family workshops
- Information on the schools' websites and itslearning

Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should fully understand the Brindishe Schools' online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.

- The Online Safety Leads will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff meetings/training sessions.
- The Online Safety Leads will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisation.
- Participation in school sessions for staff or parents (this may include attendance at assemblies/lessons).

Reducing Online Risks

At Brindishe Schools we recognise that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks.

- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.

- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.

Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices. All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. We support all our learners to be resilient online and support them to report and block harmful and unwanted content.

Learning from home

- Online safety messages are reinforced when children are expected to learn from home using the online learning platform ItsLearning.
- Teachers and support staff ensure that children have access to engaging home learning, which will be supplemented by external websites checked by the teacher before recommending.
- The Online Safety Leads will ensure that parents are given information for checking their home devices are secure and this information is available for parents when they children are spending an extended period of time online for example during a bubble lockdown.

Recording and responding to incidents

We encourage our children to be confident and ready to report inappropriate incidents involving the internet or mobile technology.

What do we do if…

- An inappropriate website is accessed unintentionally by a child or a staff member.
- An inappropriate website is accessed intentionally by a child or a staff member.

1. In all cases of inappropriate use of a website by a child or members of staff, intentionally or unintentionally, report to a senior member of staff and/or designated safeguarding lead (DSL). The Headteacher will be kept informed.
2. Inform the IT manager to ensure the site is filtered.
3. In case of inappropriate use of a website by a child, notify the parents / carers of the child.
4. In case of inappropriate use of a website by a staff member, ensure all evidence is stored and logged and addressed by the Headteacher.
5. Notify governing body where appropriate.
6. Ensure the Online Safety Leads are notified and the information is logged in the Online Safety Incident Log.

If there is a concern that a child's safety is at risk through using communication technologies (such as social networking sites or gaming), this must be reported to the DSL who will take the necessary action.

Online Sexual Violence and Sexual Harassment between Children

Brindishe Schools has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" guidance and part 5 of 'Keeping Children Safe in education'.

We recognise that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and safe-guarding policy.

Brindishe Schools recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

We also recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

Brindishe Schools will:

- Ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children

by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.

- Ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- Respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

If made aware of online sexual violence and sexual harassment, we will:

- Immediately notify the DSL (or deputy) and act in accordance with our child protection and safe-guarding policy.
- If content is contained on learner's electronic devices, manage them in accordance with the DfE 'searching screening and confiscation' advice.
- Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to partner agencies, such as Children's Services and/or the Police.

If the concern involves children and young people at a different educational setting, we will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.

If a criminal offence has been committed, the DSL (or deputy) will discuss this with the police first to ensure that investigations are not compromised.

We will review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Youth Produced Sexual Imagery ("Sexting")

Brindishe Schools recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'.

We will:

- Ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.

- Ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

- Respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.

We will not:

- View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so. If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.

- Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- Act in accordance with our child protection policies and the relevant safeguarding procedures.

- Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.

- Store the device securely. If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.

- Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.

- Inform parents and carers, if appropriate, about the incident and how it is being managed.

- Make a referral to Children's Services and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.

- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.

- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.

- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance. Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.

- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

Brindishe Schools will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

We recognise online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).

We will:

- Implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- Ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- Ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to learners and other members of our community.

If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

- Act in accordance with our child protection policies and the relevant safeguarding procedures.
- If appropriate, store any devices involved securely.
- Make a referral to Children's Services (if required/appropriate) and immediately inform the police via 101, or 999 if a child is at immediate risk.
- Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.

Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/

If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through children's services and/or the police.

If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to children's services by the DSL (or deputy).

If learners at other settings are believed to have been targeted, the DSL (or deputy) will seek support from children's services and/or the police first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

Brindishe Schools will:

- Ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- Respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- Seek to prevent accidental access to IIOC by using an internet Service provider (ISP) and by implementing appropriate filtering, firewalls and anti-spam software.

If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through children's services and/or the police.

If made aware of IIOC, we will:

- Act in accordance with our child protection policy and the relevant safeguarding procedures Store any devices involved securely.
- Immediately inform appropriate organisations.

If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported.
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the setting provided devices, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported.
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and children's services (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

- Ensure that the Head Teacher is informed in line with our managing allegations against staff policy.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
- Quarantine any devices until police advice has been sought.

Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at Brindishe Schools as noted in our 'Promoting Good Relationships' policy

Online Hate

Online hate content, directed towards or posted by, specific members of the community will not be tolerated and will be responded to in line with existing policies, including anti-bullying and behaviour.

All members of the community will be advised to report online hate in accordance with relevant policies and procedures.

The police will be contacted if a criminal offence is suspected.

If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through children's services and/or the police.

Online Radicalisation and Extremism

We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.

If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection and safeguarding policy.

If we are concerned that member of staff may be at risk of radicalisation online, the Head Teacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

Technical Infrastructure, Equipment, Filtering and Monitoring

The Brindishe Schools' IT managers will be responsible for ensuring that the schools' infrastructure and networks are as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. They will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School technical systems will be managed in ways that ensure that the Federation meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of the schools' technical systems.

- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the IT managers who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master/administrator" passwords for the school systems, used by the Network Manager must also be available to the *Headteachers/Executive Head* or other nominated senior leader and kept in a secure place.
- The IT Managers are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- There is a clear process in place to deal with requests for filtering changes.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The IT managers regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use agreement.
- Users must report any actual/potential technical incident/security breach to IT Managers and Executive Head via an email.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Children and staff are not permitted to use personal portable media for storage of images or personal information about children/staff/families.

What are we safeguarding against?

Use of Internet

Children may have access to the internet anywhere and at any time with mobile technology. Many children are carrying mobile phones, tablets and watches at a younger age than before. Therefore, the risks have increased, so it is crucial to provide a means of managing and preventing harm or compromise.

1. **Content – Where the child/adult unintentionally has access to content that is inappropriate and where perhaps using a search engine returns information that is misleading.**
2. **Contact – Where the child/person is unwittingly a participant in an online conversation/discussion, being persuaded to give out personal information and opening up the opportunity for being bullied or groomed for example.**
3. **Conduct – Where the child/person is behaving inappropriately online, or being the instigator of bullying, pretending to be someone else, or illegally downloading and sharing files.**

All staff will promote and model positive and responsible behaviours when using the internet or any digital and mobile technologies.

Email

All staff are reminded that the school email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged and from to time, monitored.
- Under no circumstances should staff contact children, parents/carers or conduct any school business using personal e-mail addresses.
- When using emails, staff will refer to children by their initials.
- Children may only use school approved accounts on the school system and only under direct school adult supervision for educational purposes.
- Staff must inform the head teacher or DSL if they receive an offensive e-mail.
- Children are not given email at Brindishe Schools.
- Members of staff are encouraged to have an appropriate work-life balance when responding to email, especially if communication is taking place between staff and parents.

Online bullying

The school will support staff and children to be aware of and understand the risks and appropriate response to online bullying by:

1. **Discussing cyberbullying** with children; how it occurs, why it occurs, and the consequences of such behaviour.
2. **Know who to report it to** in the school and how to identify other trusted adults.

The advice and support provided to children may include:

1. **Don't reply:** most of the time the bully is looking for a reaction when they're teasing or calling someone nasty names. Remind young people not to reply, if they do they're giving the bully exactly what they want.
2. **Save the evidence:** encourage young people to save the evidence of any emails or text messages they receive. This is so they have something to show when they do report the cyberbullying.
3. **Tell someone:** encourage young people to tell a trusted adult if they are being cyberbullied, and to tell them as soon as they can in order to minimise their own upset or worry.
4. **If you know that someone else is in receipt of cyberbullying, support them to report.**

Online gaming

Online gaming means you can play in real time with real people across the world through a computer, games console, tablet or smartphone connected to the internet. Games can offer children a world of adventure to immerse themselves in, but it is important to understand how children can stay safe and what games are appropriate for their age.

At Brindishe schools we will teach children to protect themselves – remind them not to share personal information and to keep gaming friends solely within the game, rather than adding them to other social networks.

Adults (parents/carers and school staff) must be aware that:

- Some games let children play and chat with anyone in the world. This means they might come across offensive language, bullying and grooming.
- Not everyone online is who they say they are. Children should avoid giving out personal details that could identify them or their location.
- Some games encourage players to buy extra elements during the game – children have been known to run up large bills without realising.
- In extreme cases bullying can be used as a tactic to win games. Children may find themselves either bullying or being bullied.

Mobile and digital devices

We recognise that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

Mobile technology devices may be school owned/provided or personally owned and might include but not limited to; tablets, games consoles and 'smart' watches and mobile phones or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage. Their use will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection and safeguarding.

Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of the community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational.

Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

Controls include:

- We do not allow learners to bring in personal devices and mobile phones except for mobile phones for those children in Y6. Any phone needs to be handed in to the school office at the beginning of the day and collected at the end of the day, and is left at the learners' own risk. Brindishe Schools has a separate mobile phone policy in place for learners and is shared with families in Year 6.
- If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place.
- Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
- Searches of mobile phone or personal devices will only be carried out in accordance with government guidelines. See www.gov.uk/government/publications/searching-screening-and-confiscation.
- Learners' mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies.
- Mobile phones and devices that have been confiscated will be released to parents or carers.
- If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.
- All members of the community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- All members of the community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

Inappropriate imagery found on children's mobile devices is a very serious issue. It must be handled sensitively, and in exact accordance with the school's child protection and safeguarding procedures.

If the images on a child's phone relate to other children and/or adults, the phone should be confiscated and advice sought from Children's Social Care who can refer the matter to the CP police. Where appropriate, the school will also alert parents/carers and any other relevant school staff e.g. DSL, class teacher, IT manager. Further guidance is available to staff at https://www.brook.org.uk/our-work/the-sexual-behaviours-traffic-light-tool

If a child reports cyber-bullying, a senior leader will ask if the child can show them the evidence of this. The adult will not look at the child's device. As appropriate, the senior leader will contact the parents/carers of the children involved.

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.

Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place during lesson time.
- Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
- Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
- Not use personal devices during teaching periods, unless permission has been given by the Head Teacher such as in emergency circumstances.
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers. Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputy) and Head Teacher.
- If a member of staff is advised to speak with a child/parent/carer using their personal mobile device (e.g. in a lockdown), staff will be asked to make their mobile number private.

Staff will not use personal devices:

- To take photos or videos of learners and will only use work-provided equipment for this purpose.
- To speak directly with learners and will only use work-provided equipment during lessons/educational activities.

If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

Visitors' Use of Personal Devices and Mobile Phones

Parents/carers and visitors (including contractors) should ensure that mobile phones are not used within the areas of school populated by learners. This is unless permission has been given e.g. at the end of performances of their own child. Use of phones linked to GDPR and Safeguarding is explained at all performances and parents/carers are asked to adhere to this.

Volunteers will have the same expectations set as staff and this is explained during their induction.

Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or Head Teacher of any breaches our policy.

Photography and Videos

Photographs and videos taken within school are used to celebrate and support learning experiences across the curriculum, to share learning with parents and carers on our school's website or itslearning platform and to provide information about the school.

The school will:

- Educate children about the risks associated with the taking, using, sharing, publishing and distributing images including on social networking sites and the importance of seeking consent before capturing someone's image.
- Allow staff to take images to support educational aims, but make sure that images or videos that include children will be selected and used carefully.
- Make sure that children's full names **will not** be used anywhere on the school website.
- Obtain written permission from parents or carers before images or videos of children are electronically published.
- Keep the written consent where children' images are used for publicity purposes, until the image is no longer in use.
- Staff **will not** keep images of children on personal devices e.g. phones or use them for any use other than in school.
- Staff using **personal devices** must not take, store, or share (with others or from a school to home device), photographs or personal or sensitive information about children or their families, this includes emails, texts or use of social media.
- Children are **not permitted to use personal digital equipment**, including mobile phones and cameras, to record images of children, staff and others without their express permission.
- Children and staff are **not permitted to use personal portable media for storage** of images (e.g., USB sticks).
- Images may be posted on the schools' website or itslearning for educational purposes as access to this material is restricted to the teaching staff and children within the confines of LGFL (London Grid for Learning)
- The IT manager has the responsibility of deleting the images when they are no longer required. At the end of the academic year, the IT manager clears existing data from the iPads and the server.
- Organisations outside the school are not permitted to take photographs or videos for external purposes without the written consent of parents or carers.

Photographs and videos taken by parents/carers

- Parents or carers are permitted to take photos or videos of their own children in school events (e.g. in concerts or performances). They are requested and reminded not to share photos/videos of school events on social networking sites, but to use them for personal and family use only as they will often include images of other children.

Social Media

Expectations

The expectations regarding safe and responsible use of social media applies to all members of Brindishe community.

The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger. All members of the community are expected to engage in social media in a positive, safe and responsible manner.

Controls include:

- All members of the community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

- We will control learner and staff access to social media whilst using school provided devices and systems on-site.

- The use of social media during school hours for personal use is not permitted. Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.

- Concerns regarding the online conduct of any member of the community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection and safeguarding policies.

Staff Personal Use of Social Media

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of Acceptable Use policy.

Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school.

Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites.
- Being aware of location sharing services.
- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Keeping passwords safe and confidential.
- Ensuring staff do not represent their personal views as that of the school.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.

Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.

Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers via Social Media

All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles.

Any pre-existing relationships or exceptions that may compromise this will be discussed with DSL and the Head Teacher. If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use official setting-provided communication tools.

Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted. Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy).

Learners' Personal Use of Social Media

Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age-appropriate sites and resources.

We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age. We will use the PEGI rating system to support our teaching of social media sites.

Any concerns regarding learners' use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools. Learners will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.

Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site or access via appropriate secure remote access systems.
- Not using portable media.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on our network.
- The appropriate use of user logins and passwords to access our network. Specific user logins and passwords will be enforced for all.
- All users are expected to log off or lock their screens/devices if systems are unattended.

Password policy

All **members of staff** will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.

All **learners** are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.

We require all users to:

- Use strong passwords for access into our system.
- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.

Managing the Safety of our Website

We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).

Controls include:

- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Learner's personal information will not be published on our website.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

Management of Applications (apps) used to Record Children's Progress

The Head Teacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of any tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

To safeguard learners' data:

- Only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.

- Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.

- Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.

- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.

- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

Publish date: Oct 2020

Next review date: Oct 2021

Devised by: The Online Safety Team

APPENDIX

For more information or links to useful resources, please see below:

UK Safer Internet Centre
https://www.saferinternet.org.uk/
Telephone: 0344 381 4772

Childnet International

Telephone: 020 7639 6967
www.saferinternet.org.uk

Telephone: 0203 770 7612
www.internetmatters.org

Useful Documentations and websites:

Department for Education Child internet safety

http://education.gov.uk/childrenandyoungpeople/safeguardingchildren/b00222029/child-internet-safety

- Online safety in schools and colleges
- Sexual imagery in schools and colleges
- Keeping Children Safe in Education statutory guidance and non-statutory
- Searching, Screening and Confiscation advice for schools
- Child Safety Online: A practical guide for parents and carers whose children are using social media

Links to other organisations or documents

There is a wealth of information available to support schools and colleges to keep children safe online. The following is not exhaustive but should provide further guidance:

www.ceop.police.uk/safety-centre/
www.thinkuknow.co.uk
www.childline.org.uk
www.disrespectnobody.co.uk
www.pshe-association.org.uk
www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation
www.education.gov.uk/ukccis
https://360safe.org.uk/
http://www.esafety-adviser.com/
http://www.esafety-adviser.com/latest-newsletter/
http://www.childnet.com/resources/digiducks-big-decision
http://www.penguinpig.co.uk/
http://www.digital-literacy.org.uk/Home.aspx
http://www.safeguardinginschools.co.uk