On-line Safety Policy

Technology and communications are rapidly changing and becoming more sophisticated, with this change comes new ways of being unsafe and feeling threatened. Online Safety (formally e-safety) has become a very important issue that is essential to address in school throughout different areas of the curriculum, to ensure that all children and adults remain safe and in control when using technology. This could be either computers or having access to the internet or through mobile telephones. This policy applies to all members of Burscough Bridge Methodist school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of the school's ICT systems. This policy seeks to ensure that the internet is used appropriately for learning but with safeguards to protect learners from harm. ALL staff and volunteers understand that children can be harmed online via hurtful and abusive messages, enticing children to engage in age inappropriate conversations, sharing and production of indecent images or encouraging risk taking behaviour

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils 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 cyberbullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. 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 Behaviour Policy.

The school 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 e-safety behaviour that take place out of school.

Vision for E-safety

At Burscough Bridge Methodist School, we aim to provide a diverse, balanced and relevant approach to ICT where security measures are balanced appropriately with effective learning and with the intention of ensuring that all children and staff are safe when using online resources. We embed our learning by following the teachings of John Wesley the founder of the Methodist Church.

.

Key Personnel

Mrs L Tyrer	Headteacher, DSL
Mrs M Murphy	Deputy DSL
Mr R Prescott	E-Safety Governor

Roles and Responsibilities

The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to all teaching staff.
The Headteacher (Designated Safeguarding Lead) is aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
The Headteacher is responsible for ensuring that all teaching staff receive suitable and regular training to enable them to carry out their e-safety roles and to train other colleagues.
The Head teacher will receive regular monitoring updates from the teaching staff
The Headteacher is trained in e-safety issues and will 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 / stranger's potential or actual incidents of grooming
• cyber-bullying

Deputy DSL

Will be a point of contact within the school for eSafety related issues and incidents.
They will work alongside the headteacher and be responsible for ensuring the development, maintenance and review of the school's eSafety policy and associated documents.

- Keep a file of signed 'acceptable use policies'
- Ensure that the policy is implemented and that compliance with the policy is actively monitored.
- Ensure all staff are aware of reporting procedures and requirements should an eSafety incident occur.
- Ensure the eSafety Incident Log is appropriately maintained on the school network and regularly reviewed together with the Headteacher
- Keep up-to-date with eSafety issues and guidance through liaison with the Local Authority School's ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- With the Headteacher provide or arrange e-Safety advice/training for staff, parents/carers and governors where needed.
- Liaise closely with the school's Designated Senior Person to ensure a co-ordinated approach across relevant safeguarding areas.

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. A member of the Governing Body will take on the role of e-Safety Governor.
The role of the E-Safety Governor will include:
• annual meetings with the e-Safety Leader
• regular monitoring of e-safety incident logs
• reporting to relevant Governors' committee

Teaching and Support Staff
Teaching and Support staff are responsible for ensuring that:
• they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
• they have read, understood and signed the Staff Acceptable Use Policy / Agreement (appendix 1)
• they report any suspected misuse or problem to the Headteacher/Deputy DSl for investigation, action or sanction
• all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
• e-safety issues are embedded in all aspects of the curriculum and other activities
• pupils understand and follow the e-safety and acceptable use policies
• pupils 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, pupils 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

Pupils:
• Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy (appendix 2)
• 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.

• They should also know and understand policies on the taking / use of images and on cyber-bullying.

• Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

• Will be consulted annually (via School Council) for feedback and input on e-Safety.

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. The school will take every opportunity to help parents understand these issues through termly e-Safety updates. These updates will give parents the knowledge of e-Safety issues and safe practices by directing them to websites, information about national and local e-safety campaigns and relevant literature. Parents/carers will also be invited to offer their views and provide feedback on e-safety for consideration by the school.

Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

E-safety across the Curriculum:

It is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond.
The three main areas of e-Safety risk are:
Content: Pupils need to be taught that not all content is appropriate or from a reliable source.
Contact: Pupils need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.
Conduct: Children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others.
Commercialism: Young people's privacy and enjoyment online can sometimes be affected by advertising and marketing schemes, which can also mean inadvertently spending money online, for example within applications. Children need to be made aware of the necessity to keep their personal information private, learn how to block both pop-ups and spam emails, turn off in-app purchasing on devices where possible and use a family email address when filling in online forms.

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children need the help and support of the school to recognise and avoid e-safety risks and build their resilience. It is essential that staff reinforce e-safety messages across the curriculum. e-Safety at Burscough Bridge will be addressed in the following ways:

- A planned e-safety curriculum is provided as part of Computing / PSHE / other lessons on a termly basis and is regularly revisited

- Key e-safety messages are reinforced as part of a planned programme of assemblies, delivered on a termly basis.

- A focus on staying safe online and cyberbullying is undertaken every year during inclusion week and will also be addressed as part of the PSHE curriculum on a termly basis.
- • Pupils 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.
- • Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- • Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement (appendix 2) and encouraged to adopt safe and responsible use both within and outside school.
- • Staff should act as good role models in their use of digital technologies the internet and mobile devices
- • Pupils should not be allowed to freely search the internet, staff should consider prior to lessons the sort of sites that should be visited and be vigilant in monitoring the content of the websites the young people visit.
- • It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs or discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study, but clear reasons for any such request should be given.

Mobile Phones and Devices:

Children:

- Children are forbidden from having mobile phones on their person whilst on school premises.
- Children must hand their mobile phones to their class teacher upon arrival at school and it is their responsibility to retrieve them at the end of the school day.
- The phone must be switched off and only switched on again when the child has left the school grounds.
- Mobile games consoles are not permitted under any circumstances
- Online bullying by pupils, via texts and emails, will be treated as seriously as any other type of bullying and will be managed through our ***Anti-bullying / Behaviour Policy***
- DfE advice; ***Searching, Screening and Confiscation*** is followed where there is a need to search a pupil for a mobile device
-

Staff:

Personal mobile phones belonging to members of staff must be switched off for the duration of the school day unless they are being used in the Staffroom or Office areas.

- Staff are permitted to have their mobile phone on their person – in a pocket or bag but they must be switched off in the school (with the exception of Staffroom and Office areas) within school hours.
- Staff must not access their mobile phone when children are present in the room.
- No images, video or audio of children is to be recorded on personal mobile phones.

- Staff may access the school's Wi-Fi on their mobile phone but for work purposes only.
- School visits and trips of the school premises- staff may be required to take their mobile phones for emergencies.
- All content and applications are purchased to comply with copyright legislation.
- Content may only be transferred to school equipment and may not be transferred to personal devices/laptops.
- Additionally, content may be placed in the school's 'cloud' storage. This is accessed through an allocated school email account and password.

Use of digital media (cameras and recording devices)

Written permission for pupil's use of and access to digital media is sought from parents when the pupil joins the school and lasts for the duration of their school life. (Home School Agreement)

Staff are to be informed by the Headteacher whose photographs may not be taken.

All images and videos of children are to be saved on the school office computer and periodically erased from school equipment.

It is requested that parents who video or photograph school events, do not post this content on social media.

Only school equipment is used by staff and pupils for all school photography and film.

Photographs of children will not be taken and stored on staff's own portable storage devices.

Staff should remain vigilant regarding visitors' use of mobile devices

Social Networks

No social network or instant messaging sites are to be accessed in school by pupils.

No social network or instant messaging sites are to be accessed by staff during teaching time and/or using school equipment.

All staff need to be aware of the following points:

- They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- Adults must not communicate with pupils using any digital technology where the content of the communication maybe considered inappropriate or misinterpreted.
- If a Social Network site is used by a staff member, details must not be shared with pupils and parents, and privacy settings must be set at maximum.
- Pupils must not be added as 'friends' on any Social Network site.
- It is not acceptable for staff to accept friend/follower requests from students who are currently enrolled at the school unless they are family members.
- Communication with past pupils, parents or siblings of pupils (not enrolled at school) is strongly discouraged particularly if the pupils are under the age of 18 years of age.
- Remember; whatever means of communication you use you should always conduct yourself in a professional manner. If content is made available on the web it is available for everyone to see and remains there forever.

Any content posted online should not:

- Bring the school into disrepute
- Lead to valid parental complaints
- Be deemed derogatory towards school and/or its employees
- Be deemed derogatory towards pupils and/or parents or carers

Parents:

- Parents should be aware that posting inappropriate comments about individual members of staff or children can be construed as online bullying. If this situation arises then the parents(s) in question will be invited into school to discuss their issues and asked to remove the offending post.
- It is not acceptable for parents to discuss issues that they may be experiencing at school on social media as it may bring the school into disrepute. It is preferred that the parent in question make an appointment with the relevant staff member so that their issue can be dealt with directly and then the offending post deleted.
- parents are aware that uploading images/video of their child alongside other children to social network sites is not acceptable unless specific permission has been obtained from the parents of the other children
- In the case of incidents on social media (outside of school hours) affecting children's behaviour or causing issues during school hours then a meeting will be arranged with the Headteacher and the Governor responsible, the child who has committed the incident and the child's parents to deal with the "spill over" into school hours.

Email

The following statements reflect safe practice in the use of email.
All users have access to Office Outlook Web Access through the Lancashire Grid for Learning service as the preferred school e-mail system.
Only official email addresses should be used to contact staff/pupils.
All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.
All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
All users are aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
All users must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature.

Preventing Extremism

The school is aware that it has a role to play to prevent radicalisation and extremism. To prevent the radicalisation of young people the school:

- Has a filtering system to block out inappropriate websites.
- A reporting system in place for both staff and pupils to keep a record of any incidents which occur.
- Has received training on awareness and prevention of extremism.
- Has AUPs in place for staff, children and anyone who may need to access the schools computers (Governors).
- Is teaching Fundamental British Values as part of the school curriculum
- Through Online Safety, teaches the children to become critical learner and so they know what is acceptable or unacceptable even though filters are in place.

The use of YouTube.com in the classroom

Children will not be able to access YouTube on classroom mobile devices or laptops. Teachers may access YouTube for teaching purposes but must thoroughly review content that they are going to use with the children before presentation to the class.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data and there is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data. Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Infrastructure and Technology
Our school subscribes to the Lancashire Grid for Learning/lightspeed Service, internet content is filtered by default. An Anti-Virus package is included in the schools subscription.

All servers, wireless systems and cabling are securely located and access is restricted.

- Critical updates and software installation involving executable files is completed by the school technician who visits fortnightly.
- Security breaches should be reported to the Headteacher

Pupil/Staff Access
Pupils access school equipment under the direction of the class teacher or support staff, who will be directed by the class teacher. All staff have an individual secure username and password and pupils log on with a class username and password.

School Websites
Parental consent is sought through the Home School Agreement and all staff are to be aware of those pupils who do not have permission to appear on the school website.
Pupils should not be identifiable in pictures with captions although newsletters may contain names of children who have achieved something such as star of the week.

Dealing with Incidents
Below is an overview of how staff are required to deal with e-Safety incidents. Appendix 5 gives a more detailed review of dealing with such incidents.
All online safety incidents must be reported to the e-Safety Leader for logging and further guidance where necessary. The e-safety report will be included in the Headteachers Report and be reviewed by Governors.

Incident	**Procedure and Sanctions**
Accidental access to inappropriate materials	Inform a trusted adult. Minimise the webpage, turn the Monitor off by closing the screen on a laptop or pressing the off button on a mobile device. Enter the details in the Incident Log and report to LGfL filtering services if necessary. Persistent 'accidental' offenders may need further disciplinary action.
Using other people's logins and passwords maliciously.	Inform HT or ICT teacher. Enter the details in the Incident Log. Additional awareness raising of eSafety issues and the AUP with individual child/class. More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy. Consider parent/carer involvement
Deliberate searching for inappropriate materials.	
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way.	

Any suspected illegal material or activity, including incidents of terrorist or extremist activity or sexting (see child protection policy), must be brought to the immediate attention of the Head

teacher (DSL) who must refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation. (IWF)

This policy will be reviewed annually to ensure conformance with current guidelines and in consultation with key stakeholders

Policy Reviewed November 2018

Policy Reviewed September 2019

.