Online Safety and Media Policy

Compiled by:	**G. Burton**
Presented to staff:	**June 2019**
Presented to Governors:	**November 2019**
Presented to Parents/Carers:	
To be reviewed:	**Every 3 years or sooner if required**
Review dates:	**November 2022**
Amendments:	**2.2** **2.4** **3.1** **3.2**

Our School Vision:

'We will be a village school which provides an outstanding, rich and broad curriculum in our caring, Christian environment. We aspire for all to reach out to the wider community, and world, as they achieve their full potential academically, socially, culturally and spiritually.'

Introduction

1.1 Our School Vision informs all aspects of school life, ensuring that we equip our children with the knowledge, skills and understanding required to engage with, and succeed in their present and future lives. As Computing and the use of the internet are now a fundamental part of our society and the world in which our children will live and work, it is imperative that online safety forms an essential part of education so that the children we teach can safely participate and achieve in a rapidly changing world.

1.2 Within Computing, Information and Communication Technology covers a wide range of resources, including web-based and mobile learning, which are constantly changing and evolving. Many of these resources enable our children to access the internet both within and outside of the classroom, for a range of different purposes. Whilst this is exciting and beneficial both within and outside of the context of education, the variety, evolution and the freedom that these internet technologies bring, open up a range of risks which users need to be aware of.

1.3 At Turton and Edgworth Primary School, we are committed to safeguarding and promoting the welfare of children and young people and expect all staff and volunteers to share this commitment. We understand our responsibility as a school to educate our children on online safety, making them aware of the acceptable uses of internet technology, teaching them appropriate behaviours and how to manage and identify risks, in and beyond the classroom.

Teaching and Learning

2.1 Within school, we endeavour to create a culture of online safety within which there is a shared responsibility from all involved e.g. Governors, staff, parents and children. Through this shared responsibility, our children understand why online safety is important but also what their responsibilities are in keeping themselves and others safe.

2.2 To promote a culture of online safety within school and to keep the key concepts of learning at the forefront of our children's minds, an Online Safety display board will be placed in the computing suite and within every classroom. Also, our 'Rules for Responsible Internet Use' will be placed in prominent places around school e.g. in children's reading records, beside each laptop,

within classrooms etc.

2.3 As a school, we believe that it is essential for the teaching of online safety to be regular and meaningful to the children and their current experiences. As a result online safety is embedded across the curriculum and we teach online safety as part of every subject when internet technologies are being used and opportunities arise.

2.4 As well as taking a cross-curricular approach towards online safety, we also teach online safety discretely within our Computing lessons. As a school we follow the 'Kapow Primary Computing' scheme which has been adapted to ensure that online safety is taught at the beginning of every half term. At the start of each year, class teachers will introduce our school SMART rules and will follow this by teaching 1 Kapow online safety lesson at the start of each half term as outline in Appendix 1.

2.5 When current online safety issues arise, we respond to these as and when they arise, educating our pupils on the dangers of specific technologies that may be encountered outside of school informally.

Managing Internet Access

3.1 Information System Security

- Our school ICT systems capacity and security will be reviewed regularly
- Anti-virus Protection Software will be updated regularly by LMG Networks
- All staff must read and sign the 'Acceptable Use Policy: Staff Information Systems Code of Conduct' before using any school ICT resource.
- Permissions for staff and children will be kept up to date; for example, if a member of staff or child leaves, their access is withdrawn.
- Parents will be asked to sign and return a consent form.

3.2 Managing Filtering

- When showing children or providing children with pre-selected sites, staff will preview the material and check that it is suited to the age and maturity of pupils.
- When children are using the internet independently e.g. for research purposes, staff will be particularly vigilant and will check that pupils are searching for and accessing relevant sites.
- If staff or pupils discover an unsuitable site, it must be reported to a member of SLT or the Computing Lead and the LA will be informed so that they can take appropriate action.
- The school will work with the **LA, DfE, the Internet Service Provider and LMG Networks** to ensure systems to protect pupils are reviewed and improved.

Password Security

4.1 In order to maintain the security and safety of the school network, password security is essential for all those using internet technologies within school, especially to those who are able to access and use pupil data. As a result, staff are expected to have secure and robust passwords which are confidential and not shared with others and are expected to change their passwords periodically.

4.2 When connected to the school network whether in school or through remote access, staff are aware that they should not access or open personal emails in order to maintain their password security and the security of our school network. Individual staff users must also ensure that when logged into the school network, they do not leave their workstation unattended. When leaving their workstation, it is the responsibility of individual staff members to lock their desktop whilst it is unattended.

4.3 Each year group, from Reception through to Year 6, are currently provided with a year group log-in username and password which they are expected to keep secure and confidential. The importance of keeping passwords private is discussed with the children each year and is revisited when necessary.

4.4 If a member of staff believes that their own or a child's password has been compromised or shared with others, they have a duty to report this to the Computing Lead or a member of SLT.

Managing Information Systems

Many current and emerging technologies offer new opportunities which can enhance teaching and learning throughout the curriculum if used effectively and purposefully. Many of these technologies are familiar to the children in a context outside of the school environment. However, before these technologies are utilised within school, their educational benefits and any potential risks will be considered and assessed. In order to minimise risk and ensure our children exploit these technologies appropriately, we manage the systems below in the following ways:

5.1 Web 2 Technologies and Social Media

- On the school network, as a result of the filtering systems in place on our internet access, we aim to deny access to social media networking sites to both pupils and staff.
- As a school, we have a school Twitter account and all staff are expected to adhere to the school's Twitter Policy when interacting with this networking site.

- Through their online safety lessons all pupils are taught to be cautious about the information they are provided with by others on these sites, understanding that Social Media provides a platform for others to provide false information.

- Pupils are taught not to give out personal details which may identify themselves or their background information to people they do not know, especially on Social Networking sites. Pupils are constantly reminded not to share information such as their name, age, school, address, passwords, phone number etc.

- As above the children are also encouraged not to share images of themselves or images that give away background information (e.g. their school badge) on these sites. Through their online safety lessons the children are taught to consider the appropriateness of these images as well as their permanence and accessibility to others once an image is uploaded to a social networking site. When the children reach Upper KS2, they will also consider how images can be altered and changed by others, so that they understand that what they see online and in other aspects of life, are not always accurate representations.

- In order to minimise risk, we educate our pupils on the importance of privacy settings when using social media sites. We encourage all children to set and maintain the maximum privacy settings advising them to deny all access to people they do not know.

- All pupils are expected to report any incidents of bullying to the school and staff are to following the Behaviour Policy accordingly when dealing with these reports.

5.2 Mobile Devices (including phones)

- As a school, we allow staff to bring their personal mobile phones and devices into school for personal use. However, these must not be visible within class and should not disrupt learning (e.g. be switched off during these times). If an important call is expected, members of staff should liaise with and inform the office staff.

- With regards to mobile devices and our pupils, the children are allowed to bring their personal mobile devices into school; however, they are not permitted to use these within the classroom or around school. These must be handed in to the office staff at the beginning of the day and then should be collected again at the end of the day.

- The school is not responsible for the loss, damage or theft of any personal mobile device.

- The use of mobile devices to send inappropriate content is prohibited and permission must be sought before these devices are used to record images or sound of any member of the school community.

5.3 Email

- The use of email provides an essential means of communication within our school but also within the world in which we live. Therefore, we know it is essential that our children are educated about email systems and that they understand how to communicate through email for different purposes and audiences.

- When teaching our children about email within school, all staff should do so using 2Email on Purple Mash which allows individual staff members to monitor and limit the emails sent and received between the children's accounts. Although it is not necessary for staff to monitor all emails, within these lessons all children should be taught how to report an email using the button provided if they feel the content of an email they receive is inappropriate or offensive. In such situations, if a member of staff deems it necessary after following the correct reporting channels, they should then monitor an individual child's emails by selecting the 'Pupil to Pupil emails require approval' tab with the 2Email settings for individual children.

- With regards to staff, the school provides all staff with their own unique email address to be used solely for school business. It is the responsibility of each individual member of staff to ensure that they keep their passwords secure and to be vigilant in monitoring their own emails for those of inappropriate materials/viruses etc.

5.4 Safe Use and Storage of Images

- As a school, with the permission of parents and careers, we allow both pupils and staff to record appropriate images and videos using school equipment including mobile devices, digital cameras, video recorders and sound recorders.
- Pupils are not permitted to use their own personal digital equipment including mobile phones and cameras, to record images or videos of others unless expressed permission has been granted by the Head Teacher.
- Any recorded images or videos of any member of the school community, whether that be an adult or child, should be safety stored on the school server.

- All images and videos taken on school devices are stored on the school server and temporarily on the recording devices used. It is the responsibility of individual members of staff to ensure that images and videos are deleted from individual devices once transferred to the school server.
- Staff are prohibited from using their own personal storage devices to store data/images e.g. USB drives, memory cards, portable hard drives, personal cameras etc.
- In situations where parents are able to take photos on their own personal devices e.g. class assemblies, sports day etc. parents will be asked to keep their devices trained upon their own child and to refrain from posting any images or videos that may contain other children on social media sites.

5.5 Published Content

- At the start of each child's school career in Reception, the permission of parents/carers is sought to allow photographs and videos of their children to be published. Where this permission is not granted, it is the responsibility of all staff to ensure that the photographs/videos of these children are not published. To support our staff in this, a full list of parental consents is provided on the server in Staff Shared and is accessible to all members of staff.
- When publishing images or videos, pupils' full names will not be used anywhere, unless permission is given.
- Where pupils' work is published either within or outside of the school grounds, we will ensure that again their full name is not used and that their identity is protected unless permission has been granted.
- Electronic communication sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- General contact details should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

5.6 Film and Mass Media

- At Turton and Edgworth Primary School children may watch parts of, or whole films with a PG rating providing the teacher has judged the content to be appropriate.
- Before showing children the above or any other mass media production e.g. podcasts or videogames, staff will preview the material and check that it is suited to the age and maturity of pupils.

Assessing Risk

6.1 The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Blackburn with Darwen LA can accept liability for the material accessed, or any consequences of Internet access. Any inappropriate access whether intentional or unintentional will be reported to a member of SLT or the computing lead and to the LA where necessary.

6.2 The school will audit ICT provision to establish if the Online Safety Policy is adequate and that its implementation is effective.

Recording and Reporting Procedures

7.1 Any incidents regarding online safety should be recorded on CPOMS and should inform the designated Online Safety Co-ordinator as well as a member of SLT or the Head Teacher and where appropriate they will inform the LA.

7.2 Serious incidents within school will be reported to the Child Protection Lead and will be dealt with in accordance with school Safeguarding and Child Protection procedures.

7.3 Any incident or complaint about staff misuse must be referred to the Head Teacher.

7.4 All pupils will be taught to do the following both within and outside of school, if they come across inappropriate content or need to report an online safety incident:

- Leave the content open on the device
- Hide the content from view of others e.g. minimise the screen/close the lid/put the device to sleep/using Hector in school etc.
- Inform a responsible adult either by taking the device to them or by bringing the adult to the device.
- Children will discuss the importance of not sharing inappropriate content with others around them before reporting this to an adult.

7.5 All pupils are expected to play an active role in reducing risk when using online devices by following the online safety rules which have been designed to protect themselves and their peers. If pupils fail to follow the rules they have been taught, then sanctions consistent with our School Behaviour Policy will be applied.

Communication Policy

8.1 A set of 'Rules for Responsible Internet Use' developed by both staff and children, will be placed in all networked rooms around school. These rules will also appear on an Online Safety display within the Computer Suite and in prominent places around school.

8.2 All staff will be given access to the Online Safety Policy on Staff Shared and its importance will be revisited regularly. When the policy is updated, any changes will be shared at a staff meeting and a new copy of the policy emailed to all staff.

8.3 Staff should be aware that internet traffic may be monitored and traced to the individual device or login. Discretion and professional conduct is essential.

8.4 The school may use monitoring software where this is available to ensure that inappropriate materials are not being stored or used on school equipment.

8.5 Parents' attention will be drawn to the Online Safety Policy in the school prospectus and on the school website. When deemed necessary, updates with regards to Online Safety will be provided to parents throughout the year.

Guarding Children against Radicalisation and Extremism

9.1 Definitions

- **Radicalisation** is defined as the act or process of making a person more radical or favouring of extreme or fundamental changes in political, economic or social conditions, institutions or habits of the mind.
- **Extremism** is defined as the holding of extreme political or religious views.

9.2 At Turton and Edgworth Primary School we are fully committed to safeguarding and promoting the welfare of all our children. As a school, we recognise that safeguarding against radicalisation and extremism is no different from safeguarding against any other vulnerability. The school has a **zero tolerance** approach to extremist behaviour for all school community members. We rely on our strong values to steer our work and ensure the pastoral care of our children protects them from exposure to negative influences.

9.3 Our school, through its training cycle is aware that the internet and in particular social media is being used as a channel to influence and in extreme cases radicalise children and young people. Furthermore we are aware that vulnerable children can be exploited and groomed by older young people and adults and will:

- Consider and discuss the threats from radicalisation and extremism
- Ensure that the understanding of radicalisation is embedded in safeguarding practice and that PREVENT coordinators (Safeguarding coordinators) are engaged and signposted.
- Consider how the threat of radicalisation through the Internet and Social Media is being addressed.

Monitoring and Reviewing

10.1 The monitoring of the standards of Online Safety and of the quality of teaching and learning in this area is the responsibility of the Computing Lead.

10.2 Monitoring is carried out by the Computing Lead in the following ways:

- Informal discussions with pupils and staff
- Supporting colleagues by keeping them informed about current developments, and providing a strategic lead and direction in this subject
- Formulating an Action Plan within which the strengths and weaknesses of Computing are outlined and areas for further development are indicated.
- Reviewing and monitoring children's work through work scrutiny/book looks
- Reviewing and monitoring teaching and learning through learning walks and observations