Balshaw's
Church Of England High School

ONLINE SAFETY POLICY

Non Sibi Sed Aliis

Your word is a lamp to my feet and a light to my path.
Psalm 119, vs 105

"All things were made through him, and without him was not any thing made that was made. " **John 1:3**

This policy document and the content contained therein remains the responsibility of the Headteacher and Governing Body of the school. No amendments can be made without their express instructions and they remain the final arbiters in any matters relating to it.

Review Date: Summer Term 2025

Next Review Date: Spring Term 2026

Reviewed By: Mrs A Wilson

APPROVED BY THE HEADTEACHER – Summer Term 2025

ONLINE SAFETY POLICY

RATIONALE

Balshaw's faces the challenge of trying to keep pace with technological change. It recognises the many opportunities available from such change: opportunities to further empower young people in their education and learning and opportunities to enhance their creativity and skills in communication. However, the school also acknowledges and seeks to protect its community against the inherent risks of the new technologies, risks which cannot always be immediately identified, given the speed of change. Overall, there is the belief that the educational and social opportunities of the new technologies far outweigh the dangers.

This Policy sets out the school's position regarding the use of social networking sites and other forms of social media. The aim of the document is to ensure that all employees are fully aware of the risks associated with using such sites and their responsibilities with regards to the safeguarding and protection of both children and themselves.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and Students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.
The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote Student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. The school has a duty of care to its Students and despite the immense educational potential of ICT, there is an unsavoury side to the internet and other current aspects of technology use on mobile devices, which it would be irresponsible to ignore. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

VALUES AND PRINCIPLES

- To promote safe and responsible use of the new technologies, both within school and in the wider lives of Students. It is recognised that young people need frequent education and guidance to embed and reinforce Online Safety messages.
- To ensure that an intrinsic part of the teaching is not only information and the building of skills but also, at an appropriate level for Student maturity and understanding, discussion of attitudes and values and the ways that new technologies can impact on the quality of personal relationships. Moral, ethical, legal, religious and cultural aspects of e-learning are addressed in this way.
- To help Students to acquire the skills for making considered, informed decisions and for accepting the responsibility for the consequences of these decisions.
- To help Students to learn how to recognise and avoid exploitation and abuse.
- To help Students access appropriate advice and support when necessary.

CONTEXT

Many of the risks outlined above reflect situations in the off-line world and this Online Safety policy links with other school policies e.g.: Behaviour for Learning, Anti-Bullying, Mobile Phone & Smartwatch, Student Acceptable Behaviour Agreement, Safeguarding & Child Protection Policy and Procedures.

As with all other risks, it is impossible to eliminate all risks completely. We aim to build Students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks and be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

GUIDELINES

- The Online Safety policy is reviewed in detail by the ICT Resources and Operations Manager, the Curriculum Leader for Business & Computing and the ICT Link Governor each year. Feedback on the work on Online Safety is sought from staff, students and parents. For example: through the letters to parents which follow the use of the 'Think U Know' resource and through the use of the Balshaw's Association as a focus group.
- E-learning takes place in both formal and informal ways. There are dedicated Computing lessons for all Students, but use of new technologies is encouraged and is intrinsic in most, if not all, subject areas. Some use lies clearly within the parameters of the school day but other use may be outside of school, for instance in the use of the internet to access information for homework or the use of Web 2.0 technologies. It is neither realistic nor practical to expect that all use can be under adult supervision, either that of adults in school or parents. Young people generally embrace new technology with enthusiasm, they generally know more about it than many adults around them and thus the aim must be to help them to develop a set of safe and responsible behaviours to support them whenever they are online.
- The school will aim to use curriculum opportunities, both in Computing and other subject areas, to provide digital literacy education, helping to teach young people to become critical and discriminating users of materials they find online and through 'direct contact' services such as e-mail, chat or social networking sites. In Computing lessons, they will be taught to be aware of the various technological approaches to minimising risk.
- The continued development of effective Online Safety strategies will involve governors, all staff, Students and parents.

- The school will work within LA and police guidelines for Online Safety and make use of support available.
- A member of the Senior Leadership Team is the designated Online Safety Co-ordinator with the aim of ensuring that policy is current and that any breaches or abuse are reported to the Headteacher and dealt with. The aim is always to be consistent and appropriate in dealing with any breaches of Online Safety, using the police when necessary.
- The SLT lead will work closely with those with more detailed day to day knowledge: ICT Resources and Operations Manager, ICT Technicians and Curriculum Leader for Business & Computing. This is to ensure that technological solutions to Online Safety support classroom practice.
- Feedback will be given to the Governors' Pastoral Sub Committee. The ICT Resources and Operations Manager will also aim to regularly review and make sure that all staff receive relevant information about any emerging Online Safety issues.
- The ICT Acceptable Behaviour Policies for staff, students, parents and visitors to the school are at the centre of good practice.
- Upon appointment all staff sign the Balshaw's ICT Acceptable Behaviour Policy and also watch the self-learn video entitled "Cyber security training for school staff" from the National Cyber Security Centre (NCSC). This is then registered to show they have watched it in line with RPA Insurance requirements.

- All staff are expected to maintain an appropriate level of professional conduct in their own ICT use both within and outside school. This includes the use of social networking sites.

- Parents sign and return an agreement that their child will comply with the Balshaw's ICT Acceptable Behaviour Policy. Students will annually sign the Acceptable Behaviour Policy before logon to the school network is permitted.
- Senior Leadership acknowledge the importance of a staff development programme that deals with both the benefits and the risks of communication technologies. Varied strategies are used in staff training, for example inclusion of this aspect in the process of induction of new staff, presentations at staff meetings and practical training from ICT staff.
- Within the context of whole school policy subject leaders will develop relevant Online Safety guidelines for their departments and record these in their departmental handbooks. These will include: embedding Online Safety in the context of that subject curriculum; setting out the procedures that departmental staff are expected to follow in particular subject locations so that Students can be suitably supervised; clear procedures for the immediate reporting of any issues of concern and review through departmental meetings.
- The rate and range of technological development have also led to increasing concerns regarding Online Safety. The pastoral team are most often the members of staff who link with parents over Online Safety issues that occur out of school time but also have knock-on effects within school. They will both individually and collectively ensure that matters are followed up via the established procedures within school to ensure consistency, suitable help to students / parents and, as far as possible, pre-empt future problems.
- All staff who use ICT in the classroom have a duty to ensure that students are reminded about appropriate behaviour on a regular basis. The main rules will be displayed in all classrooms with computers. Staff need to remember that although filtering systems are generally effective they are not completely foolproof and thus safe and responsible use of the technologies is expected at all times. Students should be regularly reminded about how to seek help and report incidents.

- There are ICT guidelines for all staff informing them of the expected professional behaviour in relation to use of the internet, school equipment and conduct beyond school. There is also specific LA Guidance on the use of social networking sites. See Appendix 4.
- School personal data is collected, stored and used according to the principles of the Data Protection Act (2018) and the General Data Protection Regulation (GDPR).

- The school reserves the right to check any ICT device in the school, including any belonging to students (or technically to their parents) if there are grounds to suspect it has been used in any way contrary to this policy.
- When using websites all staff will be mindful of the matter of copyright. Students will be encouraged to look for copyright information on sites visited, so reinforcing their understanding of this important issue.
- In production of class and homework, staff will make students aware that plagiarism is not only cheating but that, where sufficient is copied, an illegal infringement of copyright also constitutes a criminal offence.

AIMS AND OBJECTIVES OF THE POLICY

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the school's Online Safety provision. Students need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online Safety education will be provided in the following ways:

- All students sign the Balshaw's ICT Acceptable Behaviour Policy.
- A planned online safety programme will be provided as part of Computing lessons, PHSE and House and Whole School Assemblies and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. It will also regularly cover Online Bullying.
- Students in Year 7 cover a unit of work for Online Safety in the autumn term in their Computing lessons where they learn about how to stay safe online, how to recognise and deal with incidents of Online Bullying, sexting, livestreaming and how to become good digital citizens.
- Students in Year 9 cover a unit of work on Cyber Security in their Computing lessons where they learn about legal safeguards relating to computer use, the various Acts of Parliament (including the Data Protection Act 2018 and The Computer Misuse Act 1990) and their implications for computer use. They learn about the difference between data and information, social engineering including shouldering, name generator attacks, phishing and blagging. They also learn about hacking (both ethical and unethical), Denial of Service attacks (DOS and DDOS) and brute force attacks, as well as malware, including viruses, trojans, worms, adware, ransomware and spyware. Data harvesting and identity theft are also discussed together with ways of protecting online identity and privacy.
- Students in Year 9 also cover a further unit of work for Online Safety which is aimed at pupils aged 13/14, where they will learn about social media addiction, privacy, security and copyright, sexual behaviour online and health, wellbeing and lifestyle.
- The 'Think U Know' resource will be delivered to all students by their Tutors in PSHE lessons. This resource (or relevant updated program) will be used with each new Year 7 intake. The lesson(s) are followed up with a letter to parents informing them of the work done and asking that they themselves view the CEOPs website.
- Key Online Safety messages will be reinforced as part of a planned programme of assemblies e.g.: during Safer Internet Week, National Anti-Bullying Week.

- Students will 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
- Students will be helped to understand the need for the Student ABP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school. This message will be reinforced each time students access computers in school via screen log in.
- Students will be taught to reference and acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms.
- Staff should act as good role models in their use of ICT, the internet and mobile devices
- Posters and displays will be made around school to reinforce the message of staying safe on the internet.

Education – Parents / Carers

- Many Parents and Carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences.
- Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).
- Considering that Parents have a key role in creating safe ICT learning at home and outside the school environment, Balshaw's will aim to further develop strategies in working with parents in this respect and in increasing parental awareness of the messages taught in school.
- The school will therefore seek to provide information and awareness to parents and carers through:
  Letters, newsletters, website, ICT magazines and Parents evenings. Making Parents aware through information letters about how to report abuse and the misuse of technology – CEOPS.
- The school will regularly update parents with online safety concerns brought about as a result of incidents in school or brought into school in relation to particular websites or social networking sites.

Education & Training – Staff

All staff will 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. An audit of the online safety training needs of all staff will be carried out regularly by the Network Manager.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Behaviour Policies
- This Online Safety policy and its updates will be presented to and discussed by staff on staff INSET days.

Training – Governors

Governors should take part in Online Safety training awareness sessions, with particular importance for those who are members of any sub-committee involved in ICT, Online Safety, Health and Safety, Anti Bullying and Child Protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / LGfL or other relevant organisation.
- Participation in school training
- Participation in information sessions for staff or parents
- Annual training in Cyber Security using the NCSC self-learn video "Cyber security training for school staff

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It 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 ICT systems will be managed in ways that ensure that the school meets the Online Safety technical requirements outlined in the Staff Acceptable Behaviour Policy and any relevant Local Authority Online Safety Policy and guidance
- There will be reviews/audits of the safety and security of school ICT systems conducted by the ICT Resources and Operations Manager
- School filtering systems include – For our firewall and filtering we use Sophos XG firewall which has the following capabilities:

  -IWF and CTIRU lists of blocked websites feed directly into the Sophos blocked lists.
  -With Sophos web filtering, over 3,000 applications can be blocked/throttled/reported on.
  -Context aware keyword filtering.

  -We also internally use NetSupport DNA to monitor keyword strokes and phrases and cross-checking against a database of over 4500 words/phrases. Our Cloud devices are also monitored in the same way.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Resources and Operations Manager and will be reviewed by the Deputy Headteacher and ICT Forum.
- All users will be provided with a username and password by the ICT Resources and Operations Manager and ICT Assistants who will keep an up to date record of users and their usernames. Staff will be required to change their password every 90 days as part of the school Password Security Policy.
- The "master / administrator" passwords for the school ICT system, used by the ICT Resources and Operations Manager /Assistant will also be available to the Headteacher or other nominated Senior Leader
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by Virtue Technology.

-Balshaw's has provided enhanced user-level filtering through the use of the Sophos UTM filtering programme and NetSupport DNA software and Classroom.Cloud which monitors keystrokes against a database of known keywords and phrases.

- In the event of the ICT Resources and Operations Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to Virtue Technology.
- Requests from staff for sites to be removed from the filtered list will be considered by the ICT Resources and Operations Manager and/or Headteacher.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Behaviour Policy.

- Remote management tools are used by staff to control workstations and view user's activity. They will not be used on staff laptops/workstations without prior permission of the staff user.
- Users can report any actual / potential online safety incident to the ICT Resources and Operations Manager, Curriculum Leader for Business & Computing or Designated Safeguarding Leader in charge of Child Protection. The incident will be reviewed and an appropriate sanction put in place.
- Security measures provided by Sophos UTM are in place to protect the servers, firewalls, routers, wireless systems, workstations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- For the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system the ICT Resources and Operations Manager and ICT Technicians will supply a temporary passcode and all "guests" will be allowed to use the guest Wi-Fi.
- The downloading of executable files by users is blocked by ICT staff.
- Staff are not permitted any personal use on laptops and other portable devices that may be used out of school that belong to school.
- Staff can contact ICT Technicians so that they can be allowed to / be forbidden from installing programmes on school workstations / portable devices. Using NetSupport DNA, software can be packaged up and distributed to allow staff to 'pull' the software from a repository and be installed.
- Agreed guidelines are in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date anti-virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Laptop and desktop hard drives are encrypted using Windows Bitlocker

Curriculum

Online Safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students 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.
- Where students are allowed to freely search the internet, e.g. using search engines, staff should 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, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Resources and Operations Manager (and other relevant staff) 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.
- Students 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
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Students should be made aware that the playing of games on the internet is strictly forbidden and anyone caught doing so will receive an appropriate sanction

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

•When using digital images, staff will inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognize the risks attached to publishing their own images on the internet e.g. on social networking sites.

•Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

•Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

•Students must not take, use, share, publish or distribute images of others without their permission

•Photographs published on the website, prospectus, or elsewhere that include students will not be used unless written parental consent has been given.

•Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

•Student's work can only be published with the permission of the student and parents or carers.

See Mobile phone policy for more details on the use of images.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and General Data Protection Regulation (GDPR) 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.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.
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 and encrypted computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓				✓			
Use of mobile phones in lessons		✓						✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones or other camera devices		✓						✓
Use of hand held devices e.g. PDAs, PSPs	✓							✓
Use of personal email addresses in school, or on school network	✓				✓			
Use of school email for personal emails	✓				✓			
Use of chat rooms / facilities				✓				✓
Use of instant messaging	✓							✓
Use of social networking sites	✓							✓
Use of blogs	✓					✓	✓	

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the ICT Resources and Operations Manager – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Students will be taught about email safety issues, such as the risks attached to the use of personal details. They will also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material. This will be done through specific Online Safety Computing lessons and Online Safety PSHE lessons and as part of the PSHE curriculum generally
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

All staff must be aware that:

(i) they do not form on-line 'friendships' or enter into communication with parents/carers and students as this could lead to professional relationships being compromised.

(ii) On-line friendships and communication with former students should be strongly discouraged particularly if the students are under the age of 18 years.

The Department for Education document 'Guidance for Safer Working Practices for Adults Working with Children and Young people in Educational Settings (March 2009) states:-

12. Communication with Students *(including the Use of Technology)*	
In order to make best use of the many educational and social benefits of new technologies, Students need opportunities to use and explore the digital world, using multiple devices from multiple locations. It is now recognised that that e.safety risks are posed more by behaviours and values than the technology itself. Adults working in this area must therefore ensure that they establish safe and responsible online behaviours. This means working to local and national guidelines on acceptable user policies. These detail the way in which new and emerging technologies may and may not be used and identify the sanctions for misuse. Learning Platforms are now widely established and clear agreement by all parties about acceptable and responsible use is essential.	*This means that schools/services should:* *- have in place an Acceptable Behaviour policy (ABP)* *- continually self-review online safety policies in the light of new and emerging technologies* *- have a communication policy which specifies acceptable and permissible modes of communication*
Communication between Students and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should	*This means that adults should:* *- ensure that personal social*

not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny. Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to Students including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. E-mail or text communications between an adult and a child young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites. Internal e-mail systems should only be used in accordance with the school/service's policy. Further information can be obtained from http://www.education.gov.uk/	*networking sites are set at private and Students are never listed as approved contacts* *- never use or access social networking sites of Students.* *- not give their personal contact details* *to Students, including their mobile telephone number* *- only use equipment e.g. mobile phones, provided by school/service to communicate with children, making sure that parents have given* *permission for this form of communication to be used* *- only make contact with children for* *professional reasons and in accordance with any school/service policy* *- recognise that text messaging should* *only be used as part of an agreed protocol and when other forms of communication are not possible* *not use internet or web-based communication channels to send personal messages to a child/young person*

TO WHOM THIS POLICY APPLIES

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. This policy applies at all times.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students 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 cyber-bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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 online safety behaviour that take place out of school.

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**					✓
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	Pornography				✓	✓
	promotion of any kind of discrimination				✓	✓
	promotion of racial or religious hatred				✓	✓
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					✓	✓
On-line gaming (educational)			✓			
On-line gaming (non educational)					✓	
On-line gambling					✓	
On-line shopping			✓		✓	
File sharing			✓			
Use of social networking sites			✓			
Use of video broadcasting e.g. Youtube		✓				

INTERVENTION STRATEGIES

RESPONDING TO INCIDENTS OF MISUSE

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such an event the LA's guidelines should be followed. Good practice is that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

UNSUITABLE USE/INAPPROPRIATE ACTIVITY

Some internet activity e.g.: accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g.: Online bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

Students

Incidents:	Refer to Head of Department / HOH	Refer to Headteacher	Refer to Police	Refer to technical support staff for action	Inform parents / carers	Removal of network internet access	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			✓					
Unauthorised use of non-educational sites during lessons							✓	
Unauthorised use of mobile phone / digital camera / other handheld device	✓				✓			
Unauthorised use of social networking / instant messaging / personal email	✓				✓			
Unauthorised downloading or uploading of files				✓			✓	✓
Allowing others to access school network by sharing username and passwords					✓			✓
Attempting to access or accessing the school network, using another student's account				✓	✓			✓
Attempting to access or accessing the school network, using the account of a member of staff		✓			✓			✓
Corrupting or destroying the data of other users				✓	✓			✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			✓		✓			✓
Continued infringements of the above, following previous warnings or sanctions								✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓			✓			✓
Using proxy sites or other means to subvert the school's filtering system	✓			✓	✓			✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓					✓	
Deliberately accessing or trying to access offensive or pornographic material	✓	✓			✓			✓
Deliberately causing network outage/downtime	✓	✓		✓	✓	✓		✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act/GDPR					✓		✓	✓

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓		✓				✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓	✓				✓	✓	
Unauthorised downloading or uploading of files	✓	✓			✓	✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account					✓			✓
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓	✓				✓		
Deliberate actions to breach data protection or network security rules	✓	✓			✓			✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓			✓	✓		✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓				✓		✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / Students		✓			✓			✓
Actions which could compromise the staff member's professional standing	✓	✓						✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓						✓
Using proxy sites or other means to subvert the school's filtering system		✓			✓			✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓			✓	✓		✓
Deliberately accessing or trying to access offensive or pornographic material		✓		✓				
Breaching copyright or licensing regulations	✓	✓				✓		
Continued infringements of the above, following previous warnings or sanctions	✓	✓				✓	✓	✓

IMPLEMENTATION OF THE POLICY

- It is the responsibility of the Headteacher to ensure that the Online Safety Policy is implemented correctly in school and all staff follow the procedures set out in it.
- The Online Safety Policy will be reviewed annually.
- The Deputy Headteacher (Pastoral) will co-ordinate all incidents of a bullying nature regarding ICT and keep a central record.
- Heads of House/Form Tutors/Classroom Teachers will keep the Deputy Headteacher (Pastoral) informed of any incidents brought to them by students.
- All staff have a responsibility to ensure any disclosures of inappropriate use of the internet by any student are passed on to the appropriate staff.
- All new staff will receive Online Safety training
- All staff will have regular Online Safety training as part of Balshaw's CPD.

ROLES AND RESPONSIBILITIES

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

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 Welfare Committee 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.

Headteacher and Senior Leadership Team

- The Headteacher is responsible 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 Designated Senior Leader for Child Protection.
- The Headteacher / SLT are responsible for ensuring that all relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The Headteacher / SLT 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 Headteacher and another member of the Senior Leadership Team will be made aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

Business & Computing Curriculum Leader

The Business & Computing Curriculum Leader is responsible for ensuring:

- that Online Safety lessons fully meet the National Curriculum in terms of content and coverage and follow the 'Education for a Connected World' framework and the 'Teaching Online Safety in School' guidance (January 2023)
- that lessons comply with the Keeping Children Safe in Education 2024 (KCSiE) statutory guidance documentation
- that Online Safety lessons, for Year 7 and Year 9, are reviewed annually to verify that the content is up to date

- the planning and coordination of the whole school activities for Safer Internet Day which takes place annually in February

ICT Resources and Operations Manager / Technical staff:

The ICT Resources and Operations Manager and ICT Technicians are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the Online Safety technical requirements outlined in the Lancashire County Council Security Policy and Acceptable Behaviour Policy and any relevant Local Authority Online Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person. Virtue Technology and SOPHOS will monitor this.
- that he / she keeps 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 school network, Virtual Learning Environment (VLE), remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Network Manager, Headteacher, Senior Leadership Team and Curriculum Leader for Business & Computing for investigation, action and sanctions where necessary
- that monitoring software / systems are implemented and updated as agreed in school policies
- email is not regularly monitored as this is private but can be locked and investigated if needed.
- that the ICT Resources and Operations Manager keeps a log of all online safety incidents

Teaching and Support Staff

Teaching and Support staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the school Staff Acceptable Behaviour Policy (ABP)
- they report any suspected misuse or problem to the ICT Resources and Operations Manager or Headteacher for investigation, action or sanction where appropriate.
- digital communications with students via email, Virtual Learning Environment 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 school activities
- Students understand and follow the school online safety and Acceptable Behaviour Policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned students 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
- adhere to the Guidance outlined by Lancashire County Council on the Use of Social Networking Sites and Other Forms of Social Media see Appendix 4

Designated Senior Leader for Child Protection (DSL)

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

- sharing of personal data
- access to illegal and or inappropriate materials
- inappropriate on-line contact with adults or strangers
- potential or actual incidents of grooming
- cyber-bullying
- Incitement to harm based on comments on Social Networking Sites

All of the above are child protection issues through the means of technology to facilitate them happening.

Students:

- are responsible for using the school ICT systems in accordance with the Student Acceptable Behaviour Policy, which they will be expected to sign before being given access to school systems
- have a good understanding of research skills and the need to avoid copying work/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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking images and use of images inappropriately and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, school website, VLE and information about national and local Online Safety campaigns and literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student Acceptable Behaviour Policy
- accessing the school website / VLE / on-line student / Student records in accordance with the relevant school Acceptable Behaviour Policy.

MONITORING AND EVALUATING THE POLICY

As a school Balshaw's will strive to review The Online Safety Policy annually in line with good practice. The Governing Body and Headteacher and ICT Resources and Operations Manager will review reported incidents and any relevant comments from students, staff, parents and governors.

The outcomes of such reviews will be considered by all staff and appropriate amendments made to measures in school where necessary. The ICT Department, Pastoral Team and SLT will discuss Acceptable Behaviour Policy strategies and sanctions regularly at appropriate

points throughout the school year. The School Council will be involved in the reviewing of the policy annually.

This policy is fundamentally important to the health and wellbeing of all students and adults within Balshaw's community. All members of the school community have a responsibility for implementing the Online Safety Policy and Acceptable Behaviour Policy.

This Online Safety policy has been developed by a working group made up of:

- Headteacher and Senior Leadership Team
- Business & Computing Curriculum Leader
- Teachers
- Support Staff
- ICT Technical staff
- Governors
- Parents and Carers

Consultation with the whole school community has taken place through the following:

- Staff meetings
- School Council
- INSET Day
- Governors sub-committee meeting
- Parents Evening
- Balshaw's Association

OTHER RELEVANT POLICIES

- Anti-Bullying Policy
- Safeguarding & Child Protection Policy & Procedures
- Health and Safety
- Guidance on copyright and plagiarism
- Data Protection Guidelines
- Mobile Phone & Smartwatch Policy
- Behaviour for Learning Policy

Sanctions – The school reserves the right to change the policy at any time without consultation

Offence	**Sanction/Punishment**
Any form of Online Bullying	***Students will incur sanctions depending upon the severity of their actions. These will vary from Head of House detentions through to several days' inclusion or exclusion. In extreme cases of Online Bullying the school will inform the police.***
Attempting to by-pass **network security**	***These are of a more serious nature and will be dealt with by SLT.*** ***Students will incur sanctions varying from detentions through to several days' inclusion or exclusion.*** ***The police will be involved for any offence that is deemed "illegal". Fixed penalty notices will be given as appropriate. Under 16 and over 16 years carry different fines.***
Storing or using unsuitable "**scripts**" onto the network which could harm the network	
Executing or installing **programs** onto the network without permission	
Downloading **offensive** materials onto network or school equipment (images/programs, etc.)	
Accessing/using/deleting other users'/areas' files with or without permission	
Undeclared **scripts** found on **USB** drives – **harmless/**compression, etc.	***The scripts will be deleted and/or the USB drive will be banned on school machines.***
Damage to computer hardware	***In line with school policy and damage to property, repair costs will have to be paid. Business and Computing departmental detention.***
Introducing **non-copyright** materials onto network (music files, etc.)	***Deletion of files, up to exclusion for more serious cases.***
Accessing and/or storing **unsuitable images/sound files** on the internet/network	***Lose internet access for a set period of time, up to detention.***
Accessing **unsuitable sites**	***Lose internet access for a set period of time up to detention. Depending on severity, could lead to time in inclusion.***
Playing "**games**"	***Warning, Head of House detention, temporary removal of internet access.***
Inappropriate comments on social media sites, e.g. Facebook, Twitter	***Head of House or SLT detention.***
Using someone else's log-on details.	***Head of House or SLT detention.***
Accessing protected/private data and files and editing.	***Head of House or SLT detention.***

GLOSSARY OF TERMS

Web 2.0 technologies	Web-based technologies that emphasise on-line collaboration and sharing among users. Here young people are increasingly creators of digital content, using software tools to collaborate with others.

.

History of Policy

Written	**2008** The Governors' Pastoral Committee accepted this policy, though it may be subject to amendment following the further work of the Online Safety team
Reviewed:	October 2012
Re-written:	October 2013
Ratified:	March 2014
Reviewed:	October 2014
Updated :	May 2015 in light of LCC Guidance on Social Networking
Updated:	June 2017
Updated:	May 2018
Updated:	May 2019
Updated:	June 2020
Updated:	April 2021
Updated:	June 2022
Updated:	May 2023
Reviewed:	May 2024

References: South West Grid for Learning ICT Guidance

Appendices

1- Student Acceptable Behaviour Policy

2 - Staff and Volunteers Acceptable Behaviour Policy

3 – Parents/Carers ABP

4 - Guidance on the Use of Social networking Sites – Lancashire County Council

5 – Taking equipment off school site Policy

APPENDIX 1- Student Acceptable Behaviour Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Behaviour Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Behaviour Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger" when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up bandwidth capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting unless I have permission from a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will not use my personal hand held / external devices (mobile phones / USB devices etc.) in school. I understand that, if I do use my own devices in school, I will face any sanctions outlined in the school Behaviour for Learning Policy.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not use games other than educational /revision games permitted by school.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Behaviour Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Behaviour Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

Student Acceptable Behaviour Agreement Form

This form relates to the Student Acceptable Behaviour Policy (ABP), to which it is attached. Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Behaviour Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I will not use my own equipment in school e.g. mobile phones, PDAs, cameras etc.
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student	
Tutor Group	
Signed	Date

Appendix 2– Staff and Volunteer Acceptable Behaviour Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Behaviour Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Behaviour Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / Students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online Safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc.) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are

published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students / parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not disclose my personal email addresses, mobile phone number or use social networking sites for communications with students. (This includes private messaging/inboxing)
- I will not post pictures of students taken in school or on school trips on any social networking sites.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant school policy). Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Behaviour Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Behaviour Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority, disciplinary action and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

APPENDIX 3- Parent / Carer Acceptable Behaviour Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Behaviour Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of Online Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that Students will have good access to ICT to enhance their learning and will, in return, expect the Students to agree to be responsible users. A copy of the student Acceptable Behaviour Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

As the parent / carer of the above student, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, Online Safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Behaviour Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's Online Safety.

Student / Student Name	
Parent / Carers Name	
Signed	
Date	

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students and members of staff may use school provided digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media but only with prior, written consent from Parents/carers in line with the Data Protection Act / GDPR. We will also ensure that when images are published the young people cannot be identified by the use of their names.

Parents are requested to sign the permission form below to allow the school to take and use images of their children.

Permission Form

As the parent / carer of the above student, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, school events that include images of children other than my own, I will abide by these guidelines in my use of these images and seek consent from other related parties.

Student Name	
Parent / Carer's Name	
Signed	
Date	

Appendix 4 - GUIDANCE ON THE USE OF SOCIAL NETWORKING SITES AND OTHER FORMS OF SOCIAL MEDIA

LANCASHIRE COUNTY COUNCIL
CHILDREN AND YOUNG PEOPLE'S DIRECTORATE
GUIDANCE ON THE USE OF SOCIAL NETWORKING SITES AND OTHER FORMS OF SOCIAL MEDIA

Introduction

The aim of this document is to provide advice and guidance for those working with children and young people in educational settings (including volunteers) regarding the use of Social Networking Sites.

The document has been produced for Governing Bodies and Headteachers of all Schools in Lancashire and for Senior Managers and Management Committees within the County Council's centrally managed teaching services. The document has been the subject of consultation with the recognised Professional Associations and Trade Unions.

Background

The use of social networking sites such as Facebook, Twitter and MySpace is rapidly becoming the primary form of communication between friends and family. In addition there are many other sites which allow people to publish their own pictures, text and videos such as YouTube and blogging sites.

It would not be reasonable to expect or instruct employees not to use these sites which, if used with caution, should have no impact whatsoever on their role in school. Indeed, appropriate use of some sites may also have professional benefits. It is naïve and outdated however to believe that use of such sites provides a completely private platform for personal communications. Even when utilised sensibly and with caution employees are vulnerable to their personal details being exposed to a wider audience than they might otherwise have intended. One example of this is when photographs and comments are published by others without the employees consent or knowledge which may portray the employee in a manner which is not conducive to their role in school. Difficulties arise when staff utilise these sites and they do not have the knowledge or skills to ensure adequate security and privacy settings. In addition there are some cases when employees deliberately use these sites to communicate with and/or form in appropriate relationships with children and young people.

Specific Guidance

Employees who choose to make use of social networking site/media should be advised as follows:-

- That they familiarise themselves with the sites 'privacy settings' in order to
- ensure that information is not automatically shared with a wider audience than intended;

That they do not conduct or portray themselves in a manner which may:-

- bring the school into disrepute;
- lead to valid parental complaints;
- be deemed as derogatory towards the school and/or its employees;
- be deemed as derogatory towards Students and/or parents and carers;
- bring into question their appropriateness to work with children and young people.
- That they do not form on-line 'friendships' or enter into communication with parents/carers and Students as this could lead to professional relationships being compromised.
- On-line friendships and communication with former students should be strongly discouraged particularly if the students are under the age of 18 years.

(*In some cases employees in schools/services are related to parents/carers and/or students or may have formed on-line friendships with them prior to them becoming parents/carers and/or students of the school/service. In these cases employees should be advised that the nature of such relationships has changed and that they need to be aware of the risks of continuing with this method of contact. They should be advised that such contact is contradictory to the Specific Guidance points above)

Safeguarding Issues

Communicating with both current and former students via social networking sites or via other non-school related mechanisms such as personal e-mails and text messaging can lead to employees being vulnerable to serious allegations concerning the safeguarding of children and young people.

The Department for Education document 'Guidance for Safer Working Practices for Adults Working with Children and Young people in Educational Settings (March2009) states:-

12. Communication with Students *(including the Use of Technology)*

In order to make best use of the many educational and social benefits of new technologies, students need opportunities to use and explore the digital world, using multiple devices from multiple locations. It is now recognised that that Online Safety risks are posed more by behaviours and values than the technology itself. Adults working in this area must therefore ensure that they establish safe and responsible online behaviours. This means working to local and national guidelines on acceptable user policies. These detail the way in which new and emerging technologies may and may not be used and identify the sanctions for misuse. Learning Platforms are now widely established and clear agreement by all parties about acceptable and responsible use is essential.

This means that schools/services should:

- have in place an Acceptable Behaviour Policy (ABP)

- continually self-review Online Safety policies in the light of new and emerging technologies

- have a communication policy which specifies acceptable and permissible modes of communication

This means that adults should:

- ensure that personal social networking sites are set at private

Communication between students and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, emails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny. Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to students including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. E-mail or text communications between an adult and a child/young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites. Internal e-mail systems should only be used in accordance with the school/service's policy.

Further information can be obtained from: http://www.dfe.org.uk

Students are never listed as approved contacts
- never use or access social networking sites of students.
- not give their personal contact details to students, including their mobile telephone number
- only use equipment e.g. mobile phones, provided by school/service to communicate with children, making sure that parents have given permission for this form of communication to be used
- only make contact with children for professional reasons and in accordance with any school/service policy
- recognise that text messaging should only be used as part of an agreed protocol and when other forms of communication are not possible not use internet or web-based communication channels to send personal messages to a child/ young person

Recommendations

(i) That this document is shared with all staff who come into contact with children and young people, that it is retained in Staff Handbooks and that it is specifically referred to when inducting new members of staff into your school/service.
(ii) That appropriate links are made to this document with your school/services Acceptable Behaviour Policy
(iii) That employees are encouraged to consider any guidance issued by their professional association/trade union concerning the use of social networking sites
(iv) That employees are informed that disciplinary action may be taken in relation to those members of staff who choose not to follow the Specific Guidance outlined above.