SHAKESPEARE PRIMARY SCHOOL

ONLINE SAFETY POLICY

To be reviewed: Annually

To go to: Finance, General Purposes & Staffing Committee

Agreed by Governors: October 2025

Review date: September 2026

Contents

Shakespeare Primary School

Online Safety Policy

1. Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our Online Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings. The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection.

2. Our School's vision for Online Safety

The School's vision for Online Safety is to provide a diverse, balanced and relevant approach to the use of technology. Our pupils will be encouraged to maximise the benefits and opportunities that technology has to offer by following the guidelines in the Lancashire Primary Online Safety framework. We will ensure that children will learn in a safe and secure environment so that they can learn effectively. Our aim is that pupils will be equipped with the skills and knowledge to use 21st Century technology appropriately and responsibly. Pupils will be taught how to recognise the risks associated with this technology and how to deal with them, both inside and outside the school environment. All users in our school community understand the need for an Online Safety policy.

3. The role of the school's Online Safety Champion

Our Online Safety Champions are Steve Twist, Headteacher & DSL for Child Protection & Elliot Mather, Family Support Manager & Back up DSL.

The core duties/role of the Online Safety Champion includes:

- Operational responsibility to ensure the development, maintenance & review of the school's Online Safety policy & associated documents, including Acceptable Use Policies.
- Ensure that the policy is implemented & that compliance with the policy is actively monitored.
- Ensure all staff are aware of reporting procedures and requirements should an Online Safety incident occur.
- Ensure the Online Safety Incident Log is appropriately maintained and regularly reviewed.
- Keep personally up to date with Online Safety issues and guidance through liaison with Local Authority Schools' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- To provide or arrange Online Safety advice/training for staff, parents/carers and governors.
- Ensure that SMT, staff, pupils and governors are updated as necessary.
- Liaise closely with the appropriate staff in school, such as the Family Support Manager & appropriate outside agencies to ensure a co-ordinated approach across relevant safeguarding areas.

3. Policies and practices

The Online Safety policy should be read in conjunction with the following other related policies and documents:

- *Anti*-Bullying *Policy*
- *Computing Policy*
- *Child Protection Policy*
- *Safe Working Practice Policy*
- *School Data Protection Policy*
- *LCC – Guidance on the use of Social Networking Sites & other forms of Social Media (see Appendix A)*

4.1 Security and data management

This section of the policy offers clear guidance to users regarding the management of potentially sensitive data.

In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be

- **Accurate**

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

In our school, data is kept secure and all staff are informed as to what they can & cannot do with regard to data in the following ways:

- The person responsible for managing information in school is the School Business Manager (SBM).
- Relevant staff know the location of data.
- Staff with access to personal data understand their legal responsibilities.
- School will ensure that data is appropriately managed both within and outside the school environment.
- All staff are aware that they should only use approved means to access, store and dispose of confidential data.
- Staff who have remote access to school data must ensure the data remains secure by being aware of the dangers of unsecured wireless access outside school.

Mobile devices and removable media

- Data held on mobile devices and removable media, where possible, is password protected and encrypted.
- Only staff laptops containing data may be allowed to be removed from the school premises with the knowledge of the Headteacher/School Business Manager.
- All ICT equipment must be signed out via the Computing coordinator.
- Staff are aware that personal devices must not be used to access data on school systems, such as downloading email or files to a smartphone.
- The SBM ensures the risk of data loss is addressed and managed.
- The SBM follows the school's procedure for backing up data on a daily basis.
- Pupils, parents/carers and visitors will be permitted to use any mobile devise on the school premises with the school's permission.

4.2 Use of mobile devices

In our school we recognise the use of mobile devices and removable devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:

- Staff are aware that some mobile devices eg mobile phones, game consoles or net books can access unfiltered internet content.
- All devices should be virus checked before use on school systems.
- Pupils who bring their mobile phone in to school must hand it their teacher when they arrive and collect it at the end of the school day.
- Parents of any pupils who need to bring a mobile phone to school, must send a letter of permission to the school's headteacher before allowing their child to bring their device.

4.3 Use of digital media

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.

School will ensure all users are informed and educated about the risks surrounding taking, using, sharing, publishing and distributing digital media and consider the purpose for which the image will be used e g school website, brochure or display.

As photographs and video of pupils and staff are regarded as personal data in terms of The General Data Protection Act (2018), school will obtain written permission for their use from the individual and/or their parents or carers.

- Permission will be obtained from parents/carers upon the pupil entering the school.
- School will not re-use any photographs or videos after the pupil leaves without further consent being sought. These photos will be deleted from school systems one year after the pupils leave Shakespeare School.
- Full names and personal details will not be used on any digital media, particularly photographs
- Parents/carers who have been invited to attend school events and allowed to take photographs and videos, will be made aware of any conditions prior to the event in writing or verbally at the event.
- Staff recognise and understand the risks associated with publishing images, particularly in relation with the use of personal Social Networking sites.
- Staff are aware that photographs/video that are taken using school equipment must only be used for school purposes, and only accessible to the appropriate staff/pupils.
- Staff who use their own digital media device to take photographs/videos must download this on to the school's secure network as soon as possible and then delete it from their device.

- When taking photographs/video staff will ensure that all subjects are appropriately dressed and not participating in activities that could be misinterpreted.

- Staff, parents/carers and pupils will be educated in the dangers of publishing images and videos of pupils or adults on Social Networking sites or websites without consent of the persons involved.

- The guidelines for safe practice relating to the use of digital media, as outlined in the school's policy will be monitored annually by the SBM.

4.4 Communication technologies

Email:

In our school the following statements reflect our practice in the use of email.

- All staff have access to the Office 365 email system as the preferred school e-mail system & this is used for any work-related activity.
- Only official email addresses are used to contact staff.
- Only key named staff are permitted to manage confidential information.
- E-Mail communication may be routinely monitored at any time in accordance with the School's Acceptable Use Policy.
- Incidents of SPAM on school email accounts are reported to the Computing Coordinator**,** BT Lancashire Services & the Online Safety Champions.
- Threatening or offensive e-mails are reported to the Online Safety Champion & evidence collected.
- Pupils do not have individual email accounts. If required as part of curriculum work, the school technician may create accounts and manage these for the duration of a project, after which they will be closed.
- In order to study curriculum units requiring the use of e-mail by pupils, the Computing coordinator and school technician may create temporary 'in-school', 'inter school' or other secure networks.

In our school the following statements outline what we consider to be acceptable and unacceptable use of the following:

Social Networks:

All staff comply with the following:

- Personal contact details are not be given to pupils including mobile telephone numbers, details of any blogs or personal websites.
- Adults do not communicate with pupils using any digital technology, except to provide online curriculum home learning as part of Covid19 situation or through the creation of school based and school website curriculum content pages.
- All children receive regular tuition, as part of Online Safety/Computing curriculum provision & are made aware of procedures to follow in order to ensure personal safety.
- School issues, which could possibly breach school confidentiality or school policy, should not be discussed on any blog or personal websites.

Mobile telephones:

- School Office telephones are used for all school related matters.
- Mobile phones are used on educational visits.

- Children are not permitted to use mobile phones in school. Those brought into school must be handed in to the child's teacher as soon as they arrive at school.
- Specific rules, regulations & guidance are in place for non-teaching visitors.

Instant Messaging:

- Secure messaging offers valuable learning opportunities. Teacher managed group messaging (e.g. school to school/class to class) is permitted & monitored internally.
- Pupils to have restricted access to video calling as a part of carefully planned school activites (& with Headteacher permission). Video calls will only be used, under direct control of the teacher, as a class learning tool.
- When using Class Dojo children are allowed to message teachers only in the context of the work or content they post, which is also viewable by their parents.
- Parents may message teachers and vice versa through the use of Class Dojo messaging or through school email systems.

Virtual Learning Environment (VLE) / Learning Platforms:

(e.g. Class Dojo)

- Only teachers of that student's class, parents and carers connected to the particular student can see the feedback data.

- Teachers control all information they enter into Class Dojo, until a parent or student claims their student profile. Class Dojo will never sell or rent user's personally identifiable information to third parties for any reason.

- Parents and children receive private passwords to enable the Dojo App. These passwords will not be shared with third parties. Administrator access and permissions is restricted to key named staff.

- All staff are aware of the importance of ensuring online-safety when submitting items onto Dojo. Parents will only receive photographs of their own child/ren. No other children will be in photographs.

- Class stories will only include children's un-named work and classroom activities, no children will appear in class story photographs,

- Children's photographs will not appear on the Class profile picture.

- Whole class posts will not include children's individual names.

Web sites and other online publications:

- The school website is managed & monitored by a key named member of staff.
- Content uploaded to the website is carefully controlled to ensure high levels of security & adherence to AUP requirements.
- All staff are aware of the importance of ensuring online safety when submitting items for publication on the school website.
- Pupils' work is not displayed in other digital locations.

Video conferencing:

- Teams is the preferred video conferencing tool.
- Video conferencing will only take place as part of carefully planned & approved education projects (with Headteacher permission).
- Teachers will be directly responsible for managing video conferencing sessions.
- Under no circumstances will children undertake video conferencing independently.
- Video conference sessions will be monitored by staff to ensure pupil safety (e.g. use of trusted sources – schools, museums, education departments).
- Written & signed agreements will be in place prior to video conferencing sessions in order to ensure preservation of copyright, privacy and Intellectual Property Rights (IPR).
- Full training for staff will be provided prior to commencing video conferencing activities.
- Video conferencing will be managed by a teaching team, not individual staff.

Others:

Bluetooth & Infrared Technologies:

- Increasingly, Bluetooth devices will become integral to school projects & specific training will be provided.
- Bluetooth devices will be configured & password protected, especially if used away from school premises (e.g. traffic survey, beach study)
- In common with all technology usage, written permission will be secured to enable still & video capture of pupil activities.

4.5 Acceptable Use Policy (AUP)

The school actively promotes responsible, safe & courteous behaviour when accessing & using technology. Issues such as internet safety, copyright, plagiarism, online bullying & respect for others' work are addressed regularly as a part of ongoing class projects.

Staff act as positive role models & trusted adults & have signed AUP agreements.

The school has adopted the Lancashire AUP template agreement format for future AUP policy development, modification & use (see appendix).

4.6 Dealing with incidents:

Incident Log:

The school will establish an incident log to be completed to record and monitor incidents/offences **(CPOMS**). This will be audited on a regular basis by the Online Safety Champion's or other designated member of the Senior Management Team.

Illegal Offences:

Any suspected illegal material or activity will be brought to the immediate attention of the Headteacher & referred to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF) who will take responsibility for all aspects of investigation. The school recognises the importance of following correct procedures & will not conduct investigations independently.

Inappropriate Usage:

Accidental access to inappropriate materials occurs very rarely & children & adults are aware of the necessary actions to take (minimise webpage, close iPad cover and hand to a teacher, click CEOPs screen cover button & tell a trusted adult immediately). These procedures are regularly reinforced as an integral part of teaching sessions.

Details will be entered in the Incident Log on CPOMS and reported to LGfL filtering services if necessary.

Therefore, if an illegal image appears on the screen – minimise webpage, close iPad cover, click CEOPs screen cover button & report to the Headteacher/ DSL for Child Protection/Deputy for Child Protection, in order that they may contact the police.

Under no circumstances must any member of staff show another member of staff the image as this is breaking the law. Under no circumstances must any member of staff clear the computer's electronic record of web history if unacceptable content has been accessed.

5. Infrastructure and technology

The school provides & maintains an infrastructure & network that offers high levels of security.

Pupil Access:

Pupils are only permitted to access the internet & school network under the direction of the school staff. Teaching staff & Assistants are always present during periods of internet & network use. Where possible, selected sites are identified for pupil use & specific monitoring takes place when children navigate the internet more freely. Automatic filtering is in place. Children are reminded regularly about the need to be safe online. This is a key feature of Computing sessions containing on-line aspects. Staff are aware to report any issues/concerns/incidents by writing in the 'Online Safety category' found on CPOMS.

Passwords:

The school network is password protected. Staff have individual logins. Pupils in key stage one gain access through Year Group logins & key stage two pupils have individual logins - these have been agreed by Senior Managers & the Computing Coordinator. Administrator logins are available to key named staff only.

Software/hardware:

Software used in school is fully licensed & documentation is housed in secure on-site locations. The Computing Coordinator retains licences for education software. Computing hardware & software are audited annually.

Managing the network and technical support:

The network is managed by key named staff & ICT technical support provided by a service level agreement. Servers, wireless systems and cabling are securely located, and physical access is restricted. All wireless devices are security enabled & are only accessible through use of secure password logins.
Security on the network is managed by key named staff with support from the ICT technician. Review of safety & security is ongoing & critical updates automatically programmed to activate as required.
Network users have clearly defined access rights. Permissions are assigned by key named staff.

All pupils & staff are aware of the need to follow routines to preserve network security. All staff are reminded regularly that on completion of work they must log out. are activated to protect the network if machines are inadvertently left unattended.

All software is installed using only Administrator login & permissions. Staff are permitted to transfer schoolwork files to the network from portable school pen-drive & these are automatically scanned for viruses upon connection.

Staff are aware of procedures to follow if they believe that security has been breached (key named points of contact).

All teachers have a school laptop. They are aware that this is school property & can be used both on-site & at home expressly for management & teaching purposes. They are not permitted to install additional software without permission & personal files are not to be transferred to or stored on this equipment. Teachers should use only school authorised equipment in school.

Filtering and virus protection:

The school subscribes to the Lancashire Grid for Learning/CLEO Broadband Service & high-level internet content filtering is provided by default. Sophos Anti-Virus software is included in the school's subscription & this is configured to receive regular updates. On rare occasions, unsuitable content may get past the filter & pupils are taught to follow set procedures if this occurs (report instantly to staff & minimise / CEOPs button / close lid).

6. Education and Training

6.1 Online Safety across the curriculum

It is vital that pupils take responsibility of their own Online Safety. School will provide suitable Online Safety education to all pupils by considering the following:

- Regular, planned Online Safety teaching within a range of curriculum areas (using SCARF PSHE curriculum).
- Additional focus on Online Safety during the National Online Safety Awareness Week and Safer Internet day.
- Pupils are made aware of the impact of online bullying during both National Online Safety Week & National Anti-Bullying Week by the Family Support Lead. Pupils are advised how to seek help if they are affected by these issues.
- Online Safety is visited regularly through safeguarding assembly themes.

6.2 Online Safety – Raising staff awareness

- A planned formal Online Safety training for all staff takes place *annually* (in line with in school child protection/safeguarding training) to update them on their responsibilities outlined in this policy & the schools' Computing policy *& staff are updated throughout the school year as necessary*

- Headteacher/Online Safety Champions/a school representative will attend training (from a county provider/CEOP) as and when required in order that they can provide advice/guidance or training to individuals
- Staff are made aware of issues which affect their own personal safeguarding e.g. use of Social Networking sites. NO staff member can accept an invite from any pupil past (under 18 years of age) or present to 'add' them on to their friend contacts.
- Staff are expected to promote and model responsible use of ICT and digital resources
- Online Safety training is provided within an induction programme for all new staff to ensure that they fully understand the school's Online Safety Policy and the Acceptable Use Policy (AUP)
- Regular updates on Online Safety Policy, AUP, curriculum resources and general Online Safety issues are discussed in staff/team meetings throughout the school year
- Schools Anti-Bullying & Online Safety Committee meet every half term to discuss any issues/reports & feedback to the headteacher

6.3 Online Safety – Raising parents/carers awareness

'Parents/Carers often either underestimate or do not realise how often children come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.' (Byron Report, 2008)

School will offer regular opportunities for parents/carers to be informed about Online Safety. These will include the benefits and risks of using various technologies. School will do this by:

- School communications, school website e.g. Wake Up Wednesdays
- Online Safety Awareness session at least annually
- Promote external Online Safety resources/online materials as a handout to all children at National Online Safety Week & thereafter, on display in the school reception area for parents/carers & on the school website.

6.4 Online Safety – Raising Governors' awareness

The Chair of Governors has specific responsibilities for Online Safety, Computing, Child Protection and Safeguarding Children & Anti-Bullying will be required to keep themselves up to date. This may be through discussion at Governor meetings, attendance at Local Authority or staff/parent/carer meetings.

7. Standards and inspection

Greater emphasis must be placed on monitoring safeguarding procedures within our school as technology is moving forward at such a rapid pace. School will consider the following to encompass this by ensuring:

- Online Safety incidents are monitored, recorded and reviewed (see appendix 10) The schools FSL will be responsible for updating this log on CPOMS & reporting these & any recurring patterns of incidents to the Headteacher/Governors

- New technologies are risk assessed & that they are included in the Online Safety Policy where appropriate
- Online Safety Champion to make necessary any changes to this policy, following regular reported Online Safety incidents which may affect practise within school
- Online Safety Champion to make staff, parents/carers, pupils and governors informed of any changes to policy and practice throughout the school year by use of class Computing / PSHE lessons, school newsletter/website, staff/governor meetings

Appendix A (Sept 2011)

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 Councils 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, WhatsApp, Twitter, Snapchat, TikTok and Instagram 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 inappropriate 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:-

o bring the school into disrepute;

o lead to valid parental complaints;

o be deemed as derogatory towards the school and/or it's employees;

o be deemed as derogatory towards pupils and/or parents and carers;

o bring into question their appropriateness to work with children and young people.

• That they do not form online 'friendships' or enter into communication with *parents/carers and pupils as this could lead to professional relationships being compromised.

• Online friendships and communication with former pupils should be strongly discouraged particularly if the pupils are under the age of 18 years.

(*In some cases employees in schools/services are related to parents/carers and/or pupils or may have formed online friendships with them prior to them becoming parents/carers and/or pupils 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 pupils 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 (March 2009) states:-

Section 12: Communication with Pupils *(including the Use of Technology)*

To make best use of the many educational and social benefits of new technologies, pupils 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 Use Policy (AUP)

- 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 pupils 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 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 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 pupils 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.

This means that adults should:

- ensure that personal social networking sites are set at private and pupils are never listed as approved contacts

- never use or access social networking sites of pupils

- not give their personal contact details to pupils, 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 contact 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

Further information can be obtained from

http://www.education.gov.uk

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 Use 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.

This policy will be reviewed annually by the Governors' Curriculum or Finance and General Purposes Committee