Roots to grow; wings to fly. Everyone achieves their potential.

TATTENHALL PARK PRIMARY SCHOOL

We respect, we enjoy, we believe.

Online Safety

&

Acceptable Use Policy

September 2020

Scheduled review date: September 2022

Contents

1. Introduction

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

Research has shown 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 is prepared to deal with the safety challenges that the use of technology brings. The policy is organised in four main sections:

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

2. Our vision for online safety

At Tattenhall Park Primary School, we use technology, when appropriate, to enhance learning and teaching, as well as to support the daily organisation and administration tasks carried out by staff.

Keeping members of our school community safe is a priority and we expect teachers and staff to act as role models in their use of technology and abide by shared decisions reflected in our online safety policy. Children are encouraged to make appropriate decisions when using technology informed by education and online safety rules. As children are engaging with new technology both inside and outside of school, we will provide opportunities for children to understand and view online safety education as a key life skill.

Our online safety policy defines acceptable and unacceptable behaviour regarding the use of technology in school and the sanctions or procedures to be followed should a breach of security occur. It is communicated to staff, governors, pupils and parents and is updated in light of the introduction of new technologies or incidents.

3. The role of the school's online safety champion

The role of the online safety champion (Mr Cragg) in our school includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's online safety policy and associated documents, including acceptable use policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an online safety incident occur.
- Ensuring the online safety incident log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with online safety issues and guidance through liaison with the local authority school's ICT team and through advice given by national agencies such as the child exploitation and online protection centre (CEOP).
- Providing or arranging online safety advice/training for staff, parents/carers and governors.

- Ensuring the headteacher, SLT, staff, pupils and governors are updated as necessary.
- Liaising closely with the school's designated safeguarding lead (Mrs Hawkins) or deputy designated safeguarding leads (Mrs Davies and Mrs d'Albert Dodd) to ensure a co-ordinated approach across relevant safeguarding areas.

4. Policies and Practices

This online safety policy should be read in conjunction with other related policies and documents.

4.1 Security and data management

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:

- Key information / data is mapped and securely stored on the SIMS database. This is accessible only by the admin team and head teacher via the admin network using a password and username.
- CPOMS is the secure cloud based database used for recording safeguarding incidents. All staff must record incidents as they arise but only the SLT (DSL and DDSL) have access to the data via two step secure log-in.
- The head teacher has overall responsibility for managing all information.
- Staff have been informed of the location of all digital (SIMS) and paper data (locked filing drawers in office) relevant to them by the head teacher.
- Staff have been informed of their legal responsibilities with respect to principles of the Data Protection Act (1988) and ensure all data is:
    1. Accurate

2. Secure
3. Fairly and lawfully processed
4. Processed for limited purposes
5. Processed in accordance with the data subject's rights
6. Adequate, relevant and not excessive
7. Kept no longer than necessary
8. Only transferred to others with adequate protection

- Our school ensures that data is appropriately managed both within and outside the school in the following ways:
- School's equipment, including teacher laptops and ipads, must only be used for school purposes and do not contain personal information e.g. personal images, personal financial details, personal software. Computers are accessed via safe username and password and it is the responsibility of the individual to keep this secure at all times. Any breaches in security must be reported immediately to the online safety champion.
- School equipment must not be used for non-educational purposes e.g. for online gambling, dating websites, home shopping, booking holidays, social networking BOTH at home and in school.
- Staff are aware of the school's procedures for disposing of sensitive data e.g. shredding hard copies, deleting digital information, deleting usernames and passwords when children leave, deleting accounts, Pupil Profile's, PIPs, SATs information and know the personal responsible should there be any queries.
- The school's policy is to remove sensitive data prior to disposal or repair of equipment and all staff are aware of the person responsible.
- Remote access is not available to teaching staff but the Head teacher and School Business Manager have remote

access to enable working from home when circumstances make this essential.

- School data shall NOT be stored on personal equipment e.g. home computer or mobile phone.
- Staff are allowed to use personal storage devices e.g. external hard drives, pen drives in school to transfer planning and educational resources etc. but not sensitive / confidential data.
- All staff have been provided with an encrypted pen drive that is protected with a password in the event that sensitive data is needed to be transferred in this way.
- All staff have access to a personal storage space within our 'networked' hard drive and should use this as the preferred area for the backing up of data. Confidential data will be stored in individual computers as to limit access. This is password protected to ensure only staff can access this information. Staff must ensure they log out of computers when out of use.
- Personal data shared via email with outside agencies (e.g. social care, SEN team, Virtual School, HR) must be sent via Egress.

4.2 Use of mobile devices

In our school, we recognize the use of mobile devices offers a range of opportunities to extend children's learning. However, all mobile devices can only access the school's broadband internet connection if set up by the school technician. This includes school-based laptops, teacher laptops and iPads. It does not include personal phones, netbooks and other internet enabled devices. Relevant security software is installed before use.

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.

Pupil images / photos / videos

All parents / carers are asked for their permission at the start of each academic year to allow the school to use digital images / photos of their child for use within school, on the school website and in the media. Images will not be displayed if parents do not agree.

Our policy is to only use images where groups of children are involved in activities that represent the work pupils are doing, thus enabling the school to celebrate our achievements to others. To ensure our pupils' personal safety, names of pupils should not accompany images used. No names are given to the media.

We allow parents / carers to take photos of special events / school activities when invited but to not focus on any child but their own. In order to support this policy, we would ask parents / carers not to use any images of our pupils on social networking sites (i.e. Facebook). This includes any professional photos that have been purchased through the school and any photos taken during school concerts or sports events etc.

Parents' individual rights to use family pictures (not containing images of other children) on social networking sites are not affected by this, although it is advisable to consider whether images posted on any websites could be copied and / or misused.

Staff images / photos / videos

Images of staff at work are not allowed to be used on social media and can only be used in media / the school website if permission is given **for each individual** photo / image. This will be removed if staff leave their position. Photos of staff taken outside of school are not affected by this but it should be considered as to whether images on social media will bring into disrepute your integrity, as well as the potential misuse of these images.

General

Photos for school use and taken for school purpose must only be taken with school equipment and remain on school premises. When iPads leave the school premises on trips etc. all images must be stored securely on return to school. These images / videos must only be stored on school equipment in school.

Any problems with security and storage will be logged and dealt with vie training or disciplinary.

4.4 Communication technologies

Email

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

- All digital communications should be professional in tone and content via an LCC email address only.
- Email is considered a secure way of transferring data from home to school and is encouraged via a secure LCC email address.
- Staff have access to their own work email account and this will be used in correspondence with all work related activities / communications. These will be accessed via a username and password only. Personal email addresses will not be used. Email is covered by the Data Protection and Freedom of Information Act and save practise will be followed in using email to ensure confidentiality. School

email addresses may be monitored at any time in accordance with the acceptable use policy.

- Staff are able to provide their school email address to parents if they choose. This communication should remain strictly professional at all times. Otherwise phone and postal communications are acceptable practice.

Social Networks

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

Social networking sites (i.e. Facebook, Instagram, Twitter etc.) are popular amongst the adult population and young people. However, many sites do have age restriction policies where the minimum acceptable age is 13 years. Any child who sets yp or uses such a site and is below the acceptable age is in clear breach of these age-restriction policies and anyone providing false information is violating the site 'Statements of Rights'. For this reason, we would actively discourage pupils in our school using any social networking sites where these restrictions apply. Parents of pupils known using these sites will receive a letter warning of dangers of these sites to vulnerable children.

The open nature of the internet means that social networking sites can leave professionals such as teachers vulnerable if they fail to observe a few simple precautions. The below guidelines are intended not as a set of instructions, but general advice on how to avoid compromising your professional position:

- To ensure that your social networking accounts do not compromise your professional position, please ensure that your privacy settings are set correctly.

- Do not, under any circumstances, accept friend requests from a person you believe to be either a parent of a pupil at your school.
- Act in accordance with your employer's information, communication, technology (ICT) policy / suitable user and any specific guidance on the use of social networking sites.

Pupils, staff or governors who are found to be misusing websites e.g. derogatory comments or inappropriate images / language are used against other pupils, members of staff or the school, will have their internet access rights in school removed and, in serious, cases further action will be taken. Staff must also consider the security settings of these sites and if it will compromise their position in school. If this occurs, staff may be disciplined or, in extreme cases, outside agencies may become involved.

Mobile telephone:

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

- Staff are not allowed to use mobile phones in class or during lessons and should not be seen using mobile phones by children within the school setting as to set a good example. Pupils are not allowed to bring mobile devices to school and technology will be given to the either the bursar or head teacher if found on pupils. These will be returned to parents at the end of the day. If a phone is lost or stolen at school, the school takes no responsibility for these.
- Staff may take their mobile phone on trips / out of school activities to contact school in an emergency / business reasons.

- Cameras shall not be used on **private** phones / cameras etc. to record video or images of children.
- Visitors may use mobile phones to complete their job / role in school if required but all visitors are asked to turn off their phones on entry as to not disturb learning.

Instant messaging

In our school, the following statements outline what we consider acceptable and unacceptable use of instant messaging:

We do not encourage or use instant messaging other than on the school website in which secure messaging is taught and used. If an inappropriate message is sent on the school website, this is followed up and children are disciplined, parents contacted and outside agencies, if appropriate, are contacted.

Websites and other online publications

In our school, the following statements outline what we consider to be acceptable and unacceptable use of websites and other online publications:

- The school website is maintained by School Spider, the teachers, head teacher and the school bursar with relevant event information and newsletters. It is also an access point to some of our school policies.
- The school website is also used as a homework and home learning hub for pupils to access through personal username and passwords.

NB: Tattenhall Park Primary School are not responsible for information and images outside of this website. We will endeavour to add links to appropriate materials only but we cannot monitor links from these websites to new ones. We teach children about keeping safe online and would encourage parents to do the same.

All displayed photos / videos etc. are displayed in accordance with parental consent forms.

Video conferencing

In our school, the following statements outline what we consider to be acceptable and unacceptable use of video conferencing (i.e. Teams, SKYPE, Zoom etc.):

- Approval by the head teacher shall be obtained in advance of the video conference taking place. All sessions should be logged including the date, time and the name of the external organisation / person(s) taking part.
- Pupils using video conferencing equipment (e.g. for purpose of assemblies within school) should be supervised at all times.
- Al staff supervising the video conference equipment should know the procedures to follow if they are unhappy with the content of a video conference session e.g. how to stop or hang up the call.
- Copyright, privacy and intellectual property rights legislation will be breached if images, video or sound are recorded without permission.
- Children should only use school devices when video conferencing and not use personal mobile devices.

4.5 Acceptable Use Policy (AUP)

An Acceptable Use Policy (AUP) is intended to ensure that all users of technology within school will be responsible and stay safe. It should ensure that all users are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes.

AUPs are given to staff, pupils and visitors / guests and must be signed and adhered to by users before access to technology is allowed, as well as agreed to by parents.

A list of children who, for whatever reason, are not allowed to access technology should be kept in school and should be available to all staff.

Our school's AUP is regularly checked and updated as and when required by the online safety champion with the support of the SLT and school governors.

All the school community is made aware of these changes as and when required.

The use and security of usernames and passwords are included, as are acceptable and unacceptable behaviours relevant to the use and level of technology being used in school.

Users are also detailed of how we protect them from potential problems such as filtering and virus software.

Sanctions for unacceptable behaviour are also outlined for all staff, pupils, guests and governors (linked to the behaviour policy and AUP documents).

4.6 Dealing with incidents

See appendix 1 for dealing with both illegal and inappropriate incidents. All details should be logged on CPOMs and events must be reported to the online safety champion and the head / child protection officer / outside agencies will be informed where appropriate.

Incidents are monitored by the online safety champion and any reoccurring problems are addressed via SLT.

5. Infrastructure and technology

Pupil access:

Pupils have an access to a range of technology.

iPads

Pupils should only access iPads when supervised by an adult. They are told they must only access websites and apps that they have been instructed to access.

Children are able to log onto websites and apps using personal usernames and passwords and must make sure to log themselves out to avoid other users accessing their accounts. Children are instructed to immediately log out of any programs that have been left logged in by other users.

Pupils must report all problems to a member of staff and not attempt to solve them alone.

Computer network

Pupils access the student area of the network with a general student password and have access to storage space on a networked drive. They are told they must only access their own folder and children found accessing other folders will be disciplined (see the school behaviour policy / AUP).

They work under the supervision of an adult on the computers and must report all problems and not attempt to solve them alone.

Passwords

Staff and children have a separate password. Admin passwords are known only to the ICT coordinator, technician and head teacher. All school members are reminded of the importance of password and their security. If compromised, these are changed instantly.

Software / hardware

All software is licensed and up to date and licences are kept by the bursar.

Managing the network and technical support

This is done by an ICT technician for the school's main network only. The technician is the first point of contact and only them and affiliated companies are used to update or repair school computers, laptops and other devices (IPads).

Filtering and virus protection

Filtering is controlled by Cheshire West and Chester Council. This is high-level security but is not impenetrable and if incidents occur, the incident flowchart (Appendix 1) procedures must be followed.

Filtering can be controlled by the ICT technician via head permission and when this is done for educational purposed only, all children are monitored whilst using the computers and the network is returned to high- level security as soon as possible. This will only be done to access a given website usually unavailable that has been checked and verified by staff and filtering will be removed with pre-warning only.

The school uses antivirus and security software as recommended by Cheshire West and Chester Council on all computers, laptops and mobile devices.

6 Education and training

Education and training are essential components of effective online safety provision. Equipping individuals, particularly pupils, with the appropriate skills and abilities to recognize the risks and how to deal with them is fundamental. Online safety guidance is embedded within the curriculum and advantage taken of new opportunities to promote online safety.

6.1 Online safety across the curriculum

Children must be supervised when using electronic devices that have access to the internet. Online safety is taught as a distinct lesson at the beginning of every half term as a reminder of possible issues. It is then taught through all curriculum areas and children are reminded of the online safety rules and how to deal with different situations throughout these lessons.

In Key Stage 2, children are taught that online resources are subject to copyright and that the pictures, videos etc. belong to someone else or a business and we must not take without permission.

Children are given an overview of cyber bullying and its potential impact and are signposted to the relevant resources and people to help them if they require support.

Children are also taught to evaluate and check sources found online to ensure they have relevant, correct and up-to-date information, as well as the reasons this information may be incorrect.

Children are also taught to evaluate and check whether online content is appropriate or not. Any inappropriate content should be reported immediately to the ICT coordinator or head teacher.

The AUP is discussed in class and teachers ensure children understand the rules before agreeing to them. Class displays and posters promote the use of being e-safe online.

6.2 Online safety – Raising staff awareness

Staff are updated regularly with online safety issues, developments and reminders by the online safety champion who is regularly trained by the local authority to ensure they are aware of potential issues to protect both themselves and the children.

The online safety champion can give advice and can get in touch with CWAC to answer any questions.

Staff are expected to promote and encourage online safety through their teaching and set a good online safety example to the children.

New staff are given this online safety policy and are expected to sign the AUP before using school technology.

Any updates to policies etc. are discussed in staff meetings.

6.3 Online safety – Raising parents' / carers' awareness

School newsletters, government documents etc. are sent home to parents / carers with advice and updates to school policies that are available online via the school website.

6.4 Online safety – Raising governors' awareness

Governors are kept up to date with changes to technology and online safety issues and must accept the school's new online safety and AUP policy before it is issues to all staff / parents.

Governors must communicate using their school email for all official business. Documents for meetings are uploaded to Teams.

Video conferencing is used to hold remote meetings where circumstances dictate that this is a necessity.

7 Standards and inspection

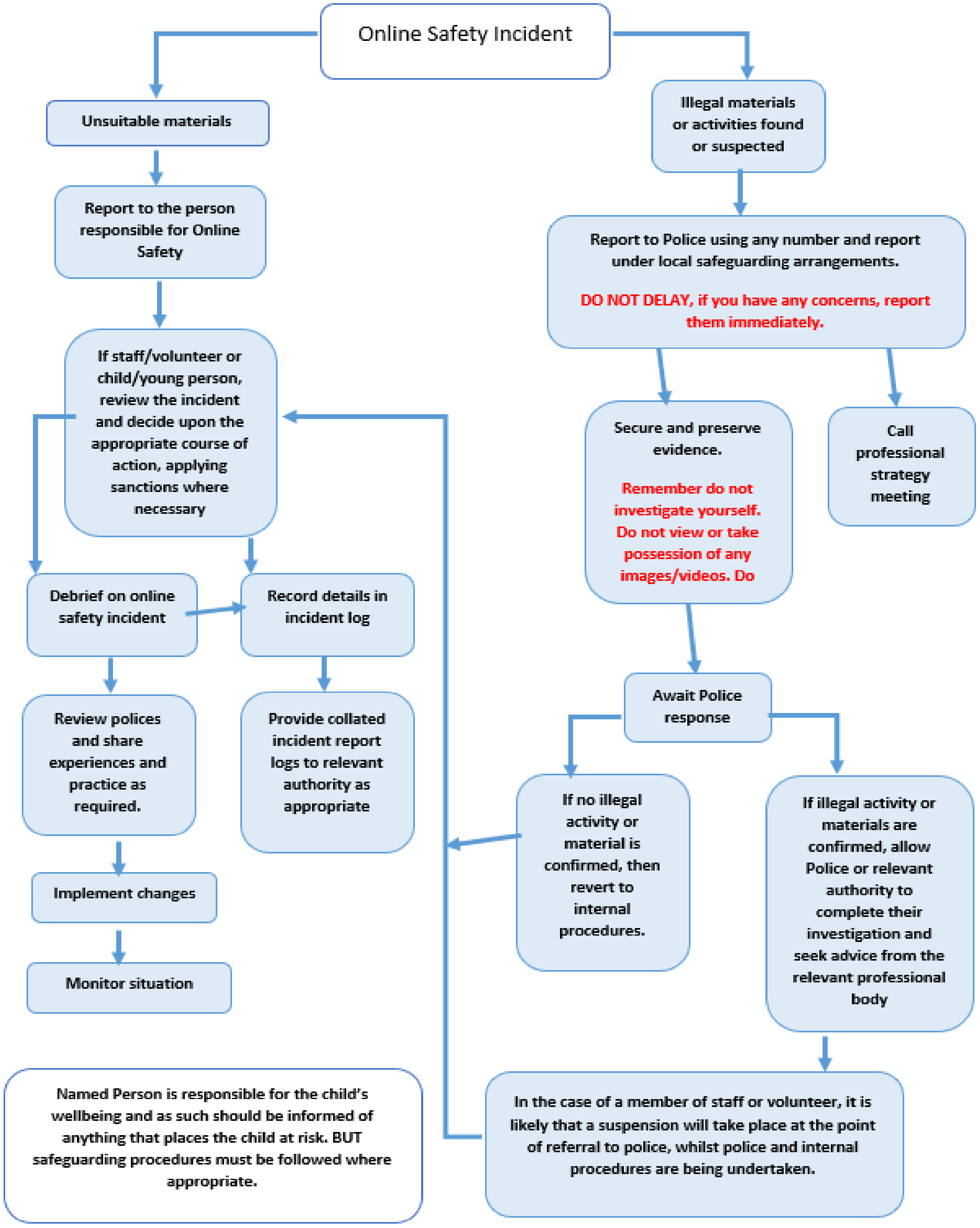
The 2011 Prevent strategy has three specific strategic objectives:

1. Respond to the ideological challenge of terrorism and the threat we face from those who promote it;
2. Prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support; and
3. Work with sectors and institutes where there are risks of radicalization that we need to address.

Prevent work depends on effective partnership.

- The school will work effectively with a range of services and partnerships.
- The school will ensure all risks are assessed.
- The school will inform the Local Safeguarding Children Board (LSCB) immediately in line with the normal safeguarding arrangements for all vulnerable pupils at risk of radicalization as evident within the school.

9. Appendix 1



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.