Monnow Primary School

E-Safety and Acceptable Use Policy

Whole – school responsibilities and acceptable use of electronic, digital and computer systems.

Updated January 2023

Introduction

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. However, use of new technologies can put young people at risk within and outside the school. The purpose of this policy is to address some of the dangers they may face, which 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.

E-Safety Personnel:

Headteacher – Miss Lisa Bowden

Deputy Headteacher – Mr Lewis Allcock

ICT/DCF Leader – Mr Dan Southgate

Responsibilities:

Headteacher

- Responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the ICT/DCF Coordinator.
- The Headteacher / Senior Leaders are responsible for ensuring that the ICT/DCF Coordinator and other relevant staff receive suitable professional learning to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff: the head teacher must be informed immediately and no further action should be taken place before this.

ICT/DCF Coordinator:

- Provide regular monitoring reports of E-safety to Senior Leadership Team
- Leads the digital leaders
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with ICT technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

- Meets regularly with Senior Leadership team to evaluate current practice and discuss any issues

Staff:

All teaching staff must ensure that they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices

- **All staff must comply with school policies on data protection and privacy to ensure that "sensitive" and "personal" data on all stakeholders remains in school.**
- All staff have read, understood and signed the school E-Safety and Acceptable Use policy.
- All staff must report any suspected misuse or problem to the ICT/DCF Coordinator Headteacher / Senior Leaders for investigation, action and consequence.
- Digital communications with students / pupils should be on a professional level and only carried out using official school systems (HWB and Google)
- E-safety issues are embedded through digital literacy units of work and wherever possible through PSD lessons
- Ensure that students / pupils understand and follow the school e-safety and acceptable use policy
- Ensure they are aware of e-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. Staff **MUST NOT** take photos of children on their personal devices and **MUST NOT** take images of children off the school premises unless on a school iPad.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use (Youtube and images) and that this policy explains the procedure for dealing with any unsuitable material that is found in internet searches

All staff should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Managing Internet Access

Information system security

- School ICT systems security is reviewed regularly.
- Virus protection is updated regularly and monitored by SRS.
- Security strategies are discussed with the LA.

E-mail

- Staff and pupils are only permitted to use authorised email accounts on the school system (HWB, Google or .Gov accounts)
- Pupil messages sent using the schools email system should not be considered private and the school reserves the right to monitor all email.
- Only staff HWB or .Gov account should be used to send and receive sensitive data with other members or the school and outside agencies.

- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school considers how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain mail or junk is not permitted.

HWB and Google Learning Environments

HWB and Google have been identified as the school's online learning environments where staff and pupils can communicate safely with each other. Staff are responsible, along with the ICT/DCF Coordinator, for ensuring that acceptable use of HWB and Google is maintained at all times. Acceptable use is as follows:

- Pupils must only log on to their own HWB and Google account at home and in school.
- Pupils must keep their login details a secret and must not share with any other pupils or persons outside the school (except parents/guardians)
- No text talk on blogs or discussions – write in full sentences and read your comments back carefully before submitting. Edit and ensure that your comments are appropriate, of a high standard and do not endanger yours or anyone else's e-safety and privacy.
- Be polite – don't post anything that could hurt anyone.
- Always show respect – be positive if you are going to comment and always remember that the blog is an extension of our school that the rest of the world is able to see.
- All posts and comments are checked by school staff before they are approved.

Twitter

The school has a central Twitter page (@Monnow_primary). The purpose of this page is to share information about school events, celebrate children's work and to share the ethos of the school with the online community. Staff will have access to the login details for the school account and are encouraged to post updates about their class regularly. When creating twitter content, staff should adhere to the following guidelines:

- Children without written photo consent are not to have their image appear anywhere online (foreground, background or from behind)
- The names of children without written consent are not to be mentioned online on the class or school Twitter accounts or website.

Published content and the school web site

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- The responsibility of providing class teachers with an up to date list of photo permission lies with the office team and these should be updated every September.
- When new pupils arrive in a class it is the class teacher's responsibility to seek photo permission if it is not already known.
- Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing at all school events.

Social networking and personal publishing

- Members of staff will not engage in dialogue about the school or with parents through the use of social networking sites.
- Pupils are not permitted to use any social networking platforms in school, with the exception of the Digital Leaders helping to compose tweets alongside staff.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- The use of **group** images on social media websites by parents represents a serious e-safety risk. We therefore require that parents DO NOT publish **group** images or videos of school events on social media websites. This would include plays, assemblies, sports day etc. If this occurs and **group** images of children are published on the internet, the safety of children will be affected. In this event, the senior leadership of the school will have to take appropriate action.
- Pupils will be advised to use nicknames and avatars when using social networking sites at home and will receive structured lessons on E-safety to support this.

Social media – Newport Local Authority Policy

- Staff should ensure they do not conduct themselves in a way that could bring the council into disrepute.
- Stagg should ensure any comments posted on social networking sites could not constitute bullying, harassment or discrimination.
- Staff must ensure their privacy settings are on the highest security level.
- Staff must consider the implications of accepting or inviting individuals connected with school as their 'friend'.
- Staff have been informed that they should not record that they work at 'Ringland Primary School' or 'Newport Council' on their Facebook page, as recommended by Newport Council.

Protecting personal data and E-privacy

All personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018. The principles sat that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Process in a way that ensures it is appropriately secure

In order to comply with this Act and ensure the privacy of all stakeholders, **the following must be followed**:

- **ALL electronic information** about a child that can show their identity should be stored securely on Hwb or on our school network. Memory sticks are discouraged but where they are used, **they must be encrypted.**
- **ALL Staff iPads** must be pass lock protected should they go missing when they are away from the school site.
- **ALL Digital Passports are to be locked away in a secure cupboard at the end of each school day.**
- **DO NOT take or even touch a phone or device a child has in their possession**. The child must be escorted to the school office and the phone placed in the safe by the child then the safe must be locked. The phone must be collected by the child at the end of the day. Phones

and personal tablets **MUST NOT** be carried by any child and they must be locked in the safe immediately on arrival at school. There may be inappropriate content e.g. pornographic images – even of children under the age of legal consent on the device – and this will be in your possession if you lay a finger on it. If you suspect that a device has inappropriate content, instruct the child to walk at your side to the Headteacher's office. Do not let the child move out of your line of sight or even handle the device as they may try to delete content.

- **DO NOT read another person's email or messages** without consent or knowledge
- **DO NOT take photos or videos without consent or awareness** – particularly with use of hidden cameras e.g. "spy" watches, badges, key fobs etc. or Google *Glass*
- **DO NOT listen in on phone calls**
- **DO NOT deliberately observe or attempt to record or memorise another person's passwords or codes**
- **DO NOT deliberately record conversations without consent**

If anyone feels that their privacy is being breached, they should inform the Headteacher in person and in private at once.

Handling offensive or inappropriate material

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network.

There are many different areas within e-safety, and as a result, breaches can often occur both accidently and deliberately. It is important all staff are aware of the potential risks certain scenarios can create. Some examples of breaches of e-safety are:

- Viewing inappropriate images/media via the internet (violent, sexual, offensive, racial, socio / economic, religious, hate)
- Making / supporting comments or opinions that are (violent, sexual, offensive, racial, socio / economic, religious, hate)
- Use of/attempting to access social media openly in front of the pupils
- Possession of mobile devices – tablets, smartphones, USB sticks, digital cameras are prohibited.
- Inappropriate use of PCs and tablets (e.g taking photographs without consent)

If a child is in involved in any breaches of the e-safety policy, the following procedures must be followed.

School PCs/Devices

If a child is found accessing inappropriate content/media at any point, please take the following actions:

On a school PC:

- Switch off the monitor, DO NOT shut down the computer.
- Instruct ALL children to leave the ICT area, and establish whether the content was accessed accidently or deliberately.
- Report to the incident to the school E-Safety officers
- Record the incident on the e-safety form (including URL/website link) and contact ICT/DCF Coordinator to block the content permanently.
- Any deliberate breaches of e-safety will be dealt with by the Headteacher as well as the e-safety officers.

- For any additional witnesses who have viewed inappropriate content, parents must be notified at once.

On a school Chromebook:

- Remove the Chromebook from the child's possession.
- Escort the child and tablet to the headteacher/deputy and provide evidence of breach of e-safety.
- Record the incident on the e-safety form (including URL/website link) and contact ICT/DCF Coordinator to block the content permanently.
- Any deliberate breaches of e-safety will be dealt with by the Headteacher as well as the e-safety officers.
- For any additional witnesses who have viewed inappropriate content, parents must be notified at once.

On a school iPad:

- Lock the iPad screen, removing it from the child's possession.
- Escort the child and tablet to the headteacher/deputy and provide evidence of breach of e-safety.
- Record the incident on the e-safety form (including URL/website link) and contact ICT/DCF Coordinator to block the content permanently.
- If a child has downloaded and accessed inappropriate apps, the iPad must then be presented to the ICT/DCF Coorindator (Mr Dan Southgate) for the app to be removed. The child will be then cautioned in the first instance and the incident recorded on the e-safety breach form.
- Any deliberate breaches of e-safety will be dealt with by the head teacher

In order to avoid any potential breaches of e-Safety amongst members of staff at Ringland Primary School, the following guidelines must be followed:

- Mobile devices (phones, personal tablets etc) must be turned off or put on silent during teaching time, and stored in a secure place (e.g. class cupboard).
- Teaching staff are not allowed to keep their device on their persons during the school day, phones may only be accessed during breaks/lunch.
- Any calls that need to be made/received must be done away from the class (e.g in staff room, office, or car), but not in corridors where children may view mobile phone use in school time as 'acceptable'.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse will be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Consequences for pupils' breach of E-safety

Step 1: For the first offence, read through the Appropriate Usage Agreement and child to re-sign and date

Step 2: Second discussion / formal warning and meet with ICT Coordinator and member of the Senior Leadership Team.

Step 3: Parents asked to come in. Sanctions imposed on child (loss of access to computers, ipads and suspension of Hwb and Google account)

Step 4 - Local police support officer to speak to children. Formal disciplinary proceedings / Headteacher to decide appropriate consequence.

Sanctions for staff breach of E-safety

The matter will be dealt with exclusively by the Headteacher.

Sexting

Many practitioners consider sexting to be 'sending or posting sexually suggestive images, including nude or semi-nude photographs, via mobiles or over the Internet.' The AWSLCP uses the following definition "Posting online or sending sexual messages or naked or semi-naked photos or video clips via any digital device"

'Youth produced sexual imagery' best describes the practice because: * 'Youth produced' includes young people sharing images that they, or another young person, have created of themselves.

* 'Sexual' is clearer than 'indecent.' A judgement of whether something is 'decent' is both a value judgement and dependent on context. * 'Imagery' covers both still photos and moving videos (and this is what is meant by reference to imagery throughout the document).

The types of incidents which this advice covers are:

• A person under the age of 18 creates and shares sexual imagery of themselves with a peer under the age of 18

• A person under the age of 18 shares sexual imagery created by another person under the age of 18 with a peer under the age of 18 or an adult

• A person under the age of 18 is in possession of sexual imagery created by another person under the age of 18.

This advice does not cover:

• The sharing of sexual imagery of people under 18 by adults as this constitutes child sexual abuse and schools should always inform the police.

• Young people under the age of 18 sharing adult pornography or exchanging sexual texts which don't contain imagery.

All incidents involving youth produced sexual imagery should be responded to in line with the school's safeguarding and child protection policy.

When an incident involving youth produced sexual imagery comes to a school or college's attention:

• the incident should be referred to the Designated Senior Person for child protection (DSP) as soon as possible

• the DSP should hold an initial review meeting with appropriate school staff. The DSP may wish to seek general advice from their School Community Police Officer.

• there should be subsequent interviews with the young people involved (if appropriate)

• parents or carers should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm

• at any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral should be made to social services and/or the police immediately in line with the school, college or other educational setting's usual arrangement.

For further guidance on procedures following 'sexting' incidents, please refer to the UKCCIS Guidance for educational settings: Sexting: Responding to incidents and safeguarding learners

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.
- E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety will be developed, including guidance from CEOP, 360' Safety and SWGfL.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.
- Annual E-safety parent presentations will be held by the ICT/DCF Coordinator and Digital Leaders in order to keep parents up to date with the latest E-safety issues and protocols.

Created: January 2023 by Dan Southgate (ICT/DCF Coordinator) and approved by the Senior Leadership Team and the Governing Body of Monnow Primary School.

Signed: _____

Chair of Governors