



E-Safeguarding Policy

(Including Mobile Device Policy)

Signed by:

Headteacher: *Dacey*

Approved Date: July 2021

Chair of Governors: Clive Brown

Approved Date: July 2021

Policy Type: Expected

Review Date: July 2022

Background

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. 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.

However, the use of these new technologies can put young people at risk within and outside the school. 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.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' 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.

The E-Safeguarding Committee

The E-Safeguarding Committee has the responsibility for issues regarding e-safeguarding and for monitoring e-safeguarding including the impact of initiatives.

Heather Lacey – Safeguarding Leader and Headteacher

Gail Whitmore – Computing Coordinator, E-Safeguarding Coordinator and Head of the E-Safeguarding Committee, PSHCE Coordinator

Leanne Kellett – Support Staff Member

Leighanne Doherty-Bedford – Governor

Tina Copley – Office Manager and ICT Technical Support link

Digital Leaders – Pupil Representation

Our school technician is Lauren Martin. The committee will consult her over technical issues related to safeguarding and security of data.

Development and review of this policy:

| | |
|---|---|
| This e-safeguarding policy was approved by the <i>Governors</i> The policy was reviewed and approved by <i>Governors</i> | October 2014 May 2015, May 2016, Sept 2017, Sept 18, Sept 19, Nov 20 |
| The implementation of this e-safeguarding policy will be monitored by the: | <i>The E-Safeguarding Committee</i> |
| Monitoring will take place at regular intervals: | <i>Annually</i> |
| The E-Safeguarding Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: | <i>September 2021</i> |

Should serious e-safety incidents take place, the following external persons/agencies should be informed:

Children's Services
Safeguarding Officer
Bradford Council
Bradford Learning
Network

Monitoring the impact of the policy

The school will monitor the impact of the policy using:

- Logs of reported incidents in the **E-Safeguarding Incident Log** and **CPOMS**
- Internal monitoring data for network activity (See Lauren Martin – school technician)
- Smoothwall user logs. We receive emails from the Bradford Learning Network which summarise user activity on our network.
- Student, staff and parent E-Safeguarding data will be gathered through the use of the Bradford Council Children's Services E-Safeguarding questionnaire available at:
www.surveymonkey.com/s/pupilesafety
www.surveymonkey.com/s/adultesafety
www.surveymonkey.com/s/parentsafety

Progress will be monitored at the start and the end of each academic year.

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safeguarding Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors in connection with the E-Safeguarding Committee. The Committee will receive regular information about e-safety incidents and monitoring reports and will pass this information onto the Governing body.

The Governor responsible for child protection (Heather Lacey) has taken on the responsibility for E-Safeguarding also, working closely with the E-Safeguarding Coordinator (Gail Whitmore).

The role of this governor will include:

- regular meetings which will include Safeguarding where safety issues will be discussed
- regular monitoring of E-Safeguarding incident logs
- regular monitoring of Smoothwall filtering through BLN emails (see Monitoring section above)
- reporting to relevant Governors and recorded through minutes

Head teacher and Senior Leaders:

- The Head teacher is responsible for ensuring the safety (including e-safeguarding) of members of the school community, though the day to day responsibility for e-safeguarding will be delegated to the E-Safeguarding Coordinator Gail Whitmore.
- The Head teacher/Senior Leaders are responsible for ensuring that the E-Safeguarding Coordinator and other relevant staff receive suitable CPD to enable them to carry out their E-Safeguarding roles and to train other colleagues, as relevant.
- The Head teacher and E-Safeguarding Coordinator are aware of the procedures to be followed in the event of a serious E-Safeguarding allegation being made against a member of staff. This is detailed in the Child Protection Policy.

E-Safeguarding Coordinator

- takes day to day responsibility for E-Safeguarding issues and has a leading role in establishing and reviewing the school E-Safeguarding policy

- ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safeguarding incident taking place
- receives reports of E-safeguarding incidents and creates a log of incidents to inform future e-safety developments
- attends the E-Safeguarding Committee (which discusses E-Safeguarding issues)
- follows the: *E-Safeguarding Officer's guide to dealing with referred incidents*. (See Appendix A)

Network Manager / Technical staff:

Lauren Martin, from *Primary Technology*, is the school technician and ensures:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that he keeps up to date with E-Safeguarding technical information and updates the E-Safeguarding/Computing Coordinator as relevant.
- that monitoring software and anti-virus software is implemented and updated

Teaching and Support Staff

Staff are responsible for ensuring that:

- they have an up to date awareness of E-Safeguarding matters and of the current school E-Safeguarding policy
- they have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the E-Safeguarding Coordinator for investigation
- digital communications with pupils (email/Virtual Learning Environment (VLE)/voice) should be on a professional level and only carried out using official school systems
- E-Safeguarding issues are embedded in all aspects of the curriculum and other school activities. E-Safeguarding lessons are taught through the *Curriculum Innovation Centre Bradford, Computing Scheme of Work*
- pupils understand and follow the school E-Safeguarding rules and have signed the *Computing Code of Conduct (Pupil AUP) and iPad AUP*
- they are aware of E-Safeguarding issues related to the use of mobile phones, cameras and hand held devices and that they implement current school policies with regard to these devices

Named person for child protection

Heather Lacey, Zoe Cooper, Gail Whitmore, Judith Carnelley and Tina Copley are the Named Persons for child protection.

They are trained in E-Safeguarding issues and are 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 (see cyber bullying section in this policy)

Children

- Pupils are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy (the Computing Code of Conduct), which they will be expected to sign before being given access to school systems. Posters of this policy are located in computing suite for regular reference to.

Parents / Carers

The school will take every opportunity to help carers/parents to understand issues related to E-Safeguarding. We will assist parents to understand key issues in the following ways:

- E -Safety presentations.
- Newsletters offer parents advice on the use of the internet and social media at home.

- Parents are asked to discuss the *Pupil Acceptable Use Policy* with their children, which is enclosed in the school admission pack. They are invited to co-sign the Pupil AUP to say they will do so.
- Parents are asked to review the letter regarding digital and video images and opt out of having images taken and or published on the school web site, Twitter and Class Dojo if they wish to do so.

Community Users

No person can log on to the internet without a user account or the internet password. A community user account with minimal privileges will be given after discussion of the sites they wish to access.

Education – Pupils

The education of pupils in E-safeguarding is an essential part of the school's E-safeguarding provision. Children and young people need the help and support of the school to recognise and avoid E-Safeguarding risks and build their resilience.

E-Safeguarding education will be provided in the following ways:

- A planned E-Safeguarding programme is delivered as part of PHSE.
- The Bradford Computing Scheme of work also highlights E-Safeguarding issues that arise in the context of computing lessons.
- Key E-Safeguarding messages are reinforced as part of a planned programme of assemblies and are mentioned in the school diary.
- Pupils are taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information. Validation of information is covered in the E-Safeguarding strand of the Bradford Computing scheme of work.
- Rules for use of computing systems will be posted in all rooms. Students will sign a class copy of the Acceptable Use Policy and it will be on display in their classroom.
- For directed searches in school, staff should direct children to Primary Safe Search or other search tools recommended in the research section of the Bradford ICT Scheme of work (login needed).
- Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information. Evaluation and cross referencing of sources is covered in the Information Literacy strand of the Bradford Computing scheme of work which the school follows.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Copyright free audio and image sources are detailed in the Media strand of the Bradford Computing scheme of work which the school follows.

Education - Staff Training

It is essential that all staff receive E-Safeguarding training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A staff meeting covering E-Safeguarding will take place annually. This will be delivered by a member of Bradford Council Children's Services Curriculum ICT Team or a member of the E-Safeguarding Committee.
- An audit of the E-Safeguarding training needs of all staff will be carried out regularly.
- All new staff should receive E-Safeguarding training as part of their induction programme, ensuring that they fully understand the school E-Safeguarding policy and Acceptable Use Policies.
- Staff will be shown the procedure to follow when illegal or inappropriate material is discovered on a device (See Appendix B)

Education - Governor Training

Governors should take part in E-Safeguarding training/awareness sessions. E-Safeguarding training will be planned for governors. This may be delivered by Bradford Children's Services consultants or by members of the E-Safeguarding Committee.

Internet Provision

The school Internet is provided by the Bradford Learning Network, a DFE accredited educational internet service provider. All sites are filtered using the Smoothwall filtering system which also generates reports on user activity.

Use of digital and video images - Photographic, Video

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images online.
- Staff are allowed to take digital/video images to support educational aims. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes unless with the permission of the Head Teacher or Computing Co-Ordinator.
- Photographs of children published on the website, Twitter or Class Dojo must not contain full names.
- Pupils' full names will not be used anywhere on a website or Class Dojo.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, Twitter or Class Dojo (see form in Appendix C)

Personal Data Protection

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 computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices such as memory sticks which have been issued to all staff through school.
- Use Galaxkey when emailing sensitive data. Galaxkey is a government certified encryption service which is used by the school to share data securely.

Passwords

All users (adults and young people) will have responsibility 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.

Passwords for new users and replacement passwords for existing users can be allocated by contacting Gail Whitmore or the school technician.

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's E-Safeguarding policy
- through the Acceptable Use Agreement

Pupils will be made aware of the school's password policy:

- in Computing and/or E-Safeguarding lessons
- through the Acceptable Use Agreement

All users (at KS1 and above) will be provided with a username and password by Gail Whitmore or the school technician. They will keep an up to date record of users and their usernames.

Cyberbullying

Please see our school Anti-bullying policy.

Cyberbullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. Examples of electronic communication are social networking

web sites and apps, texting, use of other mobile or tablet apps, email or online software. Pupils and adults who feel as if they are being bullied in any way need to talk to someone who they trust.

Staff and pupils are asked to:

- Keep any evidence of cyberbullying by taking screen captures and making a note about the time and date of any of these messages and any details about the sender
- Not forward messages to other people, this perpetuates the bullying
- Report it to a trusted adult
- Not reply to any bullying messages, this could make things worse and shows the bully that they are getting a response

The school may report serious cyber bullying incidents to the Police.

Social Media

Shirley Manor Primary Academy uses social media in the following ways:

School has a Twitter account. This is used as an information service for parents. Tweets feature dates, times and reminders.

Class Dojo is used for sharing announcements and sending messages with parents. Messages are sent and reviewed during school office hours. Photos and videos can be added to a class story by teachers. All comments are moderated by teachers.

All members of staff must keep their personal and professional lives separate on social media. Personal opinions should never be attributed to the school. See staff AUA.

The school's use of social media for professional purposes will be checked regularly by the E-Safeguarding Committee to ensure compliance with the Social Media, Data Protection, Digital Image and Video sections of the E-Safeguarding policy.

Remote Learning

With effect from October 2020, Shirley Manor Primary Academy has created a Remote Learning Policy in line with government guidance which outlines the school's approach for children that will not be attending school through choice, as a result of government guidance or due to continued shielding. It also outlines Shirley Manor Primary Academy's expectations for staff that will not be attending school due to self-isolation but that are otherwise fit and healthy and able to continue supporting with the teaching, marking and planning for children. Please refer to this policy for more details on Remote Learning. Children will access remote learning from home via Microsoft Teams/Zoom and Class Dojo. All children will be given individual sign-ons and passwords in order to use both applications. Children will be reminded of the rules around accessing these applications prior to/and during the use of these applications.

Mobile Device Policy

The aim of the Mobile Device Policy is to promote safe and appropriate practice through establishing clear and robust acceptable use guidelines. This is achieved through balancing protection against potential misuse with the recognition that mobile phones are effective communication tools - which in turn can contribute to safeguarding practice and protection.

Scope

This policy applies to all individuals who have access to personal or work-related mobile phones on site. This includes staff, volunteers, committee members, children, young people, parents, carers,

visitors and community users. This list is not exhaustive. This policy also applies to any wearable technology brought into school, for example smart watches.

Policy statement

It is recognised that it is the enhanced functions of many mobile phones that cause the most concern, and which are most susceptible to misuse. Misuse includes the taking and distribution of indecent images, exploitation and bullying. When mobiles phones are misused it can impact on an individual's dignity, privacy and right to confidentiality. Such concerns are not exclusive to children and young people; hence there is a duty to protect the needs and vulnerabilities of all.

Designated 'mobile free' areas are situated within the setting are:

- Changing areas – (classrooms whilst children are changing for activities)
- toilets

A zero-tolerance policy is in place with regards to the **use** of personal or work-related mobiles by any individual in these areas.

Procedures

Personal mobiles

Effective guidance is in place to avoid the use of mobile phones causing unnecessary disruptions and distractions within the workplace, and to ensure effective safeguarding practice is promoted to protect against potential misuse. In the interests of equality, and to further promote safety, the guidance applies to any individual who has a mobile phone on site, including children, parents and visitors, as detailed below:

Staff

Staff are permitted to have their mobile phones about their person; however, there is a clear expectation that all personal use is limited to allocated lunch and/or tea breaks.

Staff are not permitted, in any circumstance to use their phones for taking, recording or sharing images and 'mobile free' areas must be observed at all times. The exception to this rule, is when prior permission has been given by the Head Teacher or Computing Co-Ordinator e.g. school trips.

Staff must not use mobile phones in lessons. During teaching time, while on playground duty and during meetings, mobile phones will be switched off or put on 'silent' or 'discreet' mode. Except in urgent or exceptional situations, mobile phone use is not permitted during teaching time, while on playground duty and during meetings. Wearable technology should not distract from learning and should also be set to a 'discreet mode' during lesson time. In accordance with the Acceptable Use Agreement, staff should not use personal devices for photography in school. Only school cameras or devices are to be used.

Staff are not permitted to use their own personal phones for contacting children, young people and their families within or outside of the setting (with the exception of using their personal phones for emergencies whilst on school trips and during Covid 19 – ensuring that they use the 'block caller id' facility on their phones).

Pupils

Students remain responsible for all of their personal effects whilst at school. When students enter the school grounds the school takes no responsibility for mobile phones. Mobile phones are brought to school entirely at the owner's risk. The school accepts no responsibility for replacing lost, stolen or damaged mobile phones. There is no reason why a student needs to have in their possession or use a mobile phone during the day. Parents are reminded that in cases of emergency the school office remains a vital and appropriate point of contact and can ensure your child is reached quickly and assisted in any appropriate way.

School does not allow children to bring mobile phones into class. Students are advised that if they bring a mobile phone onto the school grounds during the school day, they must hand the phone in at the office before school and collect it at the end of the school day. The phones will be secured in the office and students can retrieve their phone at the end of the day (during Covid 19 these phones are handed to their class teacher who stores them safely in class). If students do bring their mobile phone to school, it should be clearly marked with their name. Parents are required to sign a form to say they agree to these rules.

As part of the digital literacy scheme of work we use, pupils are taught about the dangers of using mobile phones, the fact that location services can say exactly where you are and how quickly children can post content online before thinking about the consequences.

Parents, visitors and contractors

Parents, visitors and contractors are respectfully requested not to use their mobile phones in any of the designated mobile free areas. Should phone calls and/or texts need to be taken or made, use is restricted to those areas not accessed by children in order to avoid any unnecessary disturbance or disruption to others. Under no circumstances is **any** individual permitted to take images or make recordings on a mobile phone. Any individual bringing a personal device into the setting must ensure that it contains no inappropriate or illegal content.




Emergency contact

It is recognised that mobile phones provide direct contact to others, and at times provide a necessary reassurance due to their ease of access, particularly at stressful times. Staff, therefore, in agreed exceptional circumstances are permitted to keep the volume of their phone switched on. This is to enhance their own well-being and peace of mind, to reduce stress and worry and to enable them to concentrate more effectively on their work. Such use will be for an agreed limited period only, until any concerns or issues leading to the exceptional circumstance request have been resolved.

School's Mobile Devices

School has Apple, Android and Windows tablets. The use of these devices is covered by the computing equipment referred to in the pupil and staff acceptable use policies. In addition, children sign a tablet AUA before being allowed access to tablets. The rules are clearly present on the lock screen of the pupil iPads. Pupils know that they must not take pictures of other people without their permission. They are not allowed to download or install apps on any device. These devices are subject to the same levels of internet filtering as all the school computers accessed by children.

An (E) Safeguarding Officer's Guide to Dealing with Referred Incidents.

| | | | | | | |
|--|--|--|---|---|--|---|
| <p>Contact. A pupil has reported feeling uncomfortable after being contacted online. This may be through social networking, email, text, pogo or by other means.</p> | <p>Exposure Exposure to inappropriate images, text and media. Including but not limited to nudity, porn, race hate material.</p> | <p>Bullying Aimed at staff/pupils/parents. Including but not limited to defamatory posts on social media sites, texts, MMS, sexting, fraps, phone calls, video conferencing</p> | <p>Inappropriate Behaviour. Including but not limited to: swearing, code / insensitive comments on social media sites, email, texts.</p> | <p>Breach of Copyright Downloading and or use of copyrighted images, text, sounds and video.</p> | <p>Obsessive Behaviour This behaviour will usually take place away from the school site. It may involve playing games or chatting online for long periods of time.</p> | <p>Loss /theft of sensitive data. A laptop/ tablet/usb stick has been lost/stolen or staff email/school network has been accessed by non-authorised personnel</p> |
| <p>Inform the Headteacher immediately. The Headteacher will follow safeguarding guidelines and may contact the police or Bradford Council Safeguarding team as necessary.</p> | <p>Has the staff member who discovered the incident....</p> <ul style="list-style-type: none"> Isolated the device? Preserved the evidence? Written up the incident in the school (e) safeguarding log? | <p>See all points in the Exposure. Column.</p>  | <p>See all points in the Exposure. Column.</p>  | <p>See all points in the Exposure. Column.</p>  | <p>Obsessive behaviour may result in mood swings, being short tempered, withdrawal from friendship groups or drowsiness.</p> | <p>Report loss of equipment to the Headteacher.</p> <p>Contact the Police if property has been stolen.</p> |
| <p>If the Headteacher is not present alert the alternative named child protection person.</p> <p>Preserve evidence of attempted contact if available by taking screen shots and saving.</p> | <p>If you need to block sites or report issues with sites contact your broadband provider. (The Bradford Learning Network number is 01274 385944)</p> <p>Make sure the device is removed to a place not accessible by children. Do not use the device until the full investigation is completed and detailed in the (e) safeguarding log.</p> <p>Consult named safeguarding/child protection person in school regarding further action</p> <p>Has there been a breach of the pupil AUP? Consult HT regarding possible sanctions.</p> <p>Has there been a breach of the staff AUP? Consult HT regarding possible sanctions.</p> <p>Has any illegal activity taken place? Consult HT with regards to contacting the Police.</p> <p>Write details of all follow up actions in the school (e) Safeguarding log.</p> <p>Fort further advice contact Bradford Council's Curriculum ICT team on 01274 385944</p> | <p>Advice. Notify parents. Do not respond to posts/calls/texts. Contact social media sites and ask them to remove posts. Report abuse to phone network. Tell a trusted adult every time a call occurs and keep a record. Record an image of any further abuse. Consider asking the poster to remove the material and teach them about the impact of their actions. Consider adapting content of PHSCE / SEAL lessons and assemblies to address the problem.</p> | <p>Advice. Notify parents. Consider adapting content of PHSCE / SEAL lessons and assemblies to address the problem.</p> | <p>Advice. Notify parents. Do staff need training in the location, use and attribution of material? The Research strand of Bradford Council Curriculum Innovation Team's ICT scheme of work covers copyright and attribution of sources.</p> | <p>Advice Discuss child's behaviour with relevant staff in school, class teacher, learning mentor. Invite parents / carers in to discuss the situation. Offer advice regarding excessive gaming. See the parent section at www.thisisknow.co.uk</p> | <p>Speak to the relevant administration personnel in school regarding contacting insurers.</p> <p>Create a list of all password protected services on the device. Change all passwords.</p> <p>If person information was lost consider informing those people affected.</p> |
| <p>Consult http://cepa.police.uk/safety-centre/ and consider reporting the incident to CEOP.</p> | <p>Has there been a breach of the staff AUP? Consult HT regarding possible sanctions.</p> <p>Has any illegal activity taken place? Consult HT with regards to contacting the Police.</p> <p>Write details of all follow up actions in the school (e) Safeguarding log.</p> <p>Fort further advice contact Bradford Council's Curriculum ICT team on 01274 385944</p> | <p>Teachers who have been abused online can contact the UK Safer Internet Centre on 0844 381 4772 or email help@saferinternet.org.uk</p> | | <p>Lists of sites with copyright free/creative commons images and sound can be found at http://innovatecentres.org.uk/ to Curriculum > Primary > Sound and Music or Multimedia.</p> | <p>Consider running parental advice sessions. The presentation for parents can be found in the teachers section of www.thisisknow.co.uk. It can be delivered by teachers who have registered at the site.</p> | |
| | | | | | | |

Appendix B Actions upon discovering inappropriate or illegal material.

This short guide explains to adults in school the procedure when illegal or inappropriate material is discovered on a device.

If you suspect or discover any other (e)safeguarding incident such as individuals contacting children online, cyber bullying, inappropriate actions, breach of copyright or loss of data then consult your (e)safeguarding officer as soon as possible.

Actions upon discovering inappropriate or illegal material.

1. Remove the device from the sight of children. If it's a web site do not close any browser windows. Do not shut the device down.

2. Preserve the evidence. If the image contains child abuse do not copy it. Take screenshots of the page in question unless the image involves child abuse.

On a PC press the print screen button and paste into a word document. Save this document to a location identified by your E-Safeguarding Coordinator. Make sure the document is not stored on a device/location accessible to children.

On an iPad hold down the home key and power key at the same time to take a screenshot. Go to your photo roll and email the screenshot to a secure email (never a personal account).

3. Inform the E-Safeguarding Coordinator.

4. Write the incident in the E-Safeguarding log/CPOMS as soon as possible.

Appendix C Photograph and Video consent form

Permission for photographs and videos

Occasionally, we may take photographs of the children at our school. We may use these images in our school's prospectus or in other printed publications and marketing materials, as well as on our website and social media. We may also make video recordings for school training or other educational use.

From time to time, our school may be visited by the media who will take photographs or film footage of a visiting dignitary or other high-profile event. Pupils will often appear in these images, which may appear in local or national newspapers, or on televised news programmes.

If we use photographs of individual pupils, we will not use the full name of that child in the accompanying text or photo caption. We may include pictures of pupils and teachers that have been drawn by the pupils. We may use group or class photographs or footage with very general labels, such as 'a science lesson' or 'making Christmas decorations'. In some cases, media organisations may ask for the full name of a student if that happens we will seek consent from the parent/carer in each case.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital images.

We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately. Websites can be viewed throughout the world and not just in the United Kingdom where the law applies.

Please tick where you consent to allow us to use photographs / videos of your child

| | |
|---|--------------------------|
| Within the school premises e.g. on school displays? | <input type="checkbox"/> |
| In our school prospectus and other printed publications that we produce for promotional purposes? | <input type="checkbox"/> |
| On our website? | <input type="checkbox"/> |
| On schools DoJo? | <input type="checkbox"/> |
| On social media e.g., Twitter? | <input type="checkbox"/> |
| To appear in the media, such as the local press? | <input type="checkbox"/> |

| | | |
|----------------------|--------|------|
| Name of parent/carer | Signed | Date |
|----------------------|--------|------|

Appendix D Parent AUP

PARENTS/CARERS

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign an Acceptable Use Policy to show that the Computing and E-Safeguarding Rules have been understood and agreed.

This Acceptable Use Policy is intended to ensure:

- that pupils will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school/academy 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 e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

Acceptable Use Policy Agreement

A copy of the Pupil Acceptable Use 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

Parent/Carers Name

Pupil Name

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

(KS1 and KS2):

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

(EYFS):

I understand that the school has discussed the Acceptable Use Agreement rules with my son/daughter and that they have received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – 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 computer systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use 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 e-safeguarding.

Signed


Date

COMPUTING ACCEPTABLE USE POLICY FOR PUPILS


THE SHIRLEY MANOR COMPUTING CODE OF CONDUCT FOR (KS2)

To ensure that pupils are fully aware of their safety when using technology and to make pupils aware of the responsibilities they have when using information systems and communicating online, they are asked to read and sign this Acceptable Use Policy. This signature shows that they have understood and agreed to our code of conduct. Pupils are asked to consult our KS1 and KS2 e-Safety rules for further information and guidance.


SHIRLEY MANOR PRIMARY ACADEMY HAS COMPUTER MONITORING FACILITIES IN OPERATION AT ALL TIMES. THESE FACILITIES INCLUDE INDIVIDUAL COMPUTER MONITORING AND INTERNET FILTERING.



| | |
|----|---|
| 1 | I understand that access to computers, the internet and email is provided to help learning. |
| 2 | I will respect computing equipment and behave appropriately with it at all times. |
| 3 | I will remember to always sit in my allocated seat in the computing suite. |
| 4 | I accept that I am responsible for any and all activity carried out under my user name. |
| 5 | I will ask permission before using the internet and will use the search engine: <i>Safe Search</i> , unless otherwise instructed. |
| 6 | I will keep my computer passwords secret and I will only log on using my own username. |
| 7 | My public messages e.g. blogging and emails will be polite and responsible. |
| 8 | I will report any unpleasant material or messages to a trusted adult. |
| 9 | I will never give out personal information online. |
| 10 | I will never arrange to meet anyone I don't know in person. |
| 11 | I will not open emails from unknown senders. |
| 12 | I will not enter the computing suite without permission. |
| 13 | I will not take or consume any food or drink in the computing room. |
| 14 | I will not use headphones, USB slots or CDROM drives without permission. |
| 15 | I will not tamper with anyone else's machine and I will leave the wires and locks alone. |
| 16 | I will not download software or inappropriate files onto the school network. |



If any of the above rules are not complied to, the school will take strict discipline action which could include the following:

- 
- 1) The incident will be logged in the incident file
 - 2) Referral filled out by teacher and given to Mrs Lacey
 - 3) Parents informed by staff
 - 4) Access to the internet blocked for 1 week
 - 5) Account/computing privileges removed

I have read, understood and agree to follow the *Computing Code of Conduct*.

Name: _____ Year group: _____ Date: _____

COMPUTING ACCEPTABLE USE POLICY FOR PUPILS
THE SHIRLEY MANOR COMPUTING CODE OF CONDUCT (KS1)

To ensure that pupils are fully aware of their safety when using technology and to make them aware of the responsibilities they have when using information systems and communicating online, they are asked to read and sign this Acceptable Use Policy. This signature shows that they have understood and agreed to our code of conduct. Pupils are asked to consult our KS1 and KS2 e-Safety rules for further information and guidance. SHIRLEY MANOR PRIMARY ACADEMY HAS COMPUTER MONITORING FACILITIES IN OPERATION AT ALL TIMES. THESE FACILITIES INCLUDE INDIVIDUAL COMPUTER MONITORING AND INTERNET FILTERING.

| | |
|----|--|
| 1 | I will behave and look after computing equipment. |
| 2 | I will always sit in my place for computing. |
| 3 | I will only use my user name to log in. |
| 4 | I will keep my passwords secret. |
| 5 | I will only use the internet when an adult is with me. |
| 6 | I will be polite on the internet. |
| 7 | I can click on the buttons and links when I know what they do. |
| 8 | I will tell my teacher if I see upsetting things on the internet. |
| 9 | I will always ask if I need help. |
| 10 | I will not share personal information online. |
| 11 | I will not enter the computing suite without an adult. |
| 12 | I will not 'LOG ON' until I am asked and I will 'LOG OFF' when told. |
| 13 | I will not use headphones or disk drives without permission. |
| 14 | I will not touch anyone else's machine and I will leave the wires and locks alone. |



If any of the above rules are not complied to, the school will take strict discipline action which could include the following:

- 1) The incident will be logged in the e-safety incident file
- 2) Referral filled out by teacher and given to Mrs Lacey
- 3) Parents informed by staff
- 4) Access to the internet blocked for 1 week
- 5) Account/computing privileges removed






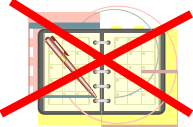
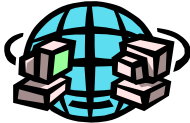
I have read, understood and agree to follow the *Computing Code of Conduct*.

Name: _____ Year group: _____ Date: _____

COMPUTING ACCEPTABLE USE POLICY FOR PUPILS THE SHIRLEY MANOR COMPUTING CODE OF CONDUCT (EYFS)

E-Safeguarding is promoted from an early age at Shirley Manor Primary. Children are asked to comply with computing rules to make sure that they are aware of their safety when using ICT resources. Parents are encouraged to discuss E-Safety with their children and are asked to sign this agreement on behalf of their children.

SHIRLEY MANOR PRIMARY ACADEMY HAS COMPUTER MONITORING FACILITIES IN OPERATION AT ALL TIMES. THESE FACILITIES INCLUDE INDIVIDUAL COMPUTER MONITORING AND INTERNET FILTERING.

| | |
|---|--|
| 1 | <p>I will look after computing equipment.</p> <div style="display: flex; justify-content: space-around; align-items: center;">   </div> |
| 2 | <p>I will be polite on the internet.</p> <div style="text-align: center;">  </div> |
| 3 | <p>I will share computing equipment.</p> <div style="text-align: right;">  </div> |
| 4 | <p>I will tell my teacher if I see upsetting things on the internet.</p> <div style="text-align: left;">  </div> |
| 5 | <p><u>I will not</u> tell strangers my name or my age.</p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  </div> <div style="text-align: center;">  </div> </div> |

I have read and agree to follow the *Computing Code of Conduct*.

Name of Parent/Guardian: _____

Name of Child: _____



IPAD RULES



- 1 Always use two hands to carry the iPad.
- 2 No liquids around the iPad.
- 3 Never change the settings on the iPad.
- 4 Keep the cover on the iPad at all times.
- 5 Never hit or slam the iPad.
- 6 Clean hands when using the iPad.
- 7 Put the iPad to sleep when listening to others.
- 8 Share the iPad nicely with others.
- 9 Do not modify someone else's work on the iPad.
- 10 Always ask permission before taking photos of others.

I have read, understood and agree to follow the *iPad Code of Conduct*.

Name: _____ Year group: _____ Date: _____