Patcham Junior School's Online Safety (e-Safety) Policy 2016

Patcham Junior School's Online Safety (e–Safety) Policy 2016

Contents

1. Creating an Online Safety Ethos

1.1 Aims and policy scope

Patcham Junior School believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles.

Patcham Junior School identifies that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

Patcham Junior School has a duty to provide the school community with quality Internet access to raise education standards, promote pupil achievement, support professional work of staff and enhance the schools management functions. Patcham Junior School also identifies that with this there is a clear duty to ensure that children are protected from potential harm online.

The purpose of Patcham Junior School online safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that Patcham Junior School is a safe and secure environment.
- Safeguard and protect all members of Patcham Junior School community online.
- Raise awareness with all members of Patcham Junior School community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This policy applies to all staff including the governing body, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop or mobile phone.

This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including computing, Personal Social Health and Education (PSHE), Citizenship and Sex and Relationships education (SRE).

1.2 Key responsibilities of the community

1.2.1 Key responsibilities of the school/setting management team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- Supporting the online safety (e-Safety) lead in the development of an online safety culture within the setting.
- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety.

- To ensure that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the school community and ensuring that the filtering and school network system is actively monitored.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- Taking responsibility for online safety incidents and liaising with external agencies as appropriate.
- Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice.
- Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices.
- To work with and support technical staff in monitoring the safety and security of schools systems and networks.
- To ensure a member of the Governing Body) is identified with a lead responsibility for supporting online safety.

1.2.2 Key responsibilities of the designated safeguarding/online safety lead are:

- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.
- Keeping up-to-date with current research, legislation and trends.
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- Work with the school/setting lead for data protection and data security to ensure that practice is in line with legislation.
- Maintaining an online safety incident/action log to record incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- Monitor the school/settings online safety incidents to identify gaps/trends and update the education response to reflect need and to report to the school management team, Governing Body and other agencies as appropriate.
- Liaising with the local authority and other local and national bodies as appropriate.
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other procedures on a regular basis (at least annually) with stakeholder input.
- Ensuring that online safety is integrated with other appropriate school policies and procedures.

1.2.3 Key responsibilities of staff are:

- Contributing to the development of online safety policies.
- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of school/setting systems and data.
- Having an awareness of online safety issues, and how they relate to the children in their care.
- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives.
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern, and taking appropriate action by working with the designated safeguarding lead.

- Knowing when and how to escalate online safety issues, internally and externally.
- Being able to signpost to appropriate support available for online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.

1.2.4. Additional responsibilities for staff managing the technical environment are:

- Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the online safety lead and DSL.
- Ensuring that the use of the setting's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the online safety lead and DSL.
- Report any breaches or concerns to the Designated Safeguarding Lead and leadership team and together ensure that they are recorded on the e Safety Incident Log, and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Providing technical support and perspective to the online safety lead and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.

1.2.5 Key responsibilities of children and young people are:

- Contributing to the development of online safety policies.
- Reading the school/setting Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.2.6. Key responsibilities of parents and carers are:

- Reading the school/setting Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of new and emerging technology.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.

2. Online Communication and Safer Use of Technology

2.1 Managing the school/setting website

The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.

The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.

The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

2.2 Publishing images and videos online

The school will ensure that all images are used in accordance with the school image use policy.

In line with the schools image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

2.3 Managing email

Pupils may only use school provided email accounts for educational purposes.

All members of staff are provided with a specific school email address to use for any official communication.

The use of personal email addresses by staff for any official school business is not permitted.

The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.

Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.

Members of the school community must immediately tell a designated member of staff if they receive offensive communication and this should be recorded in the school online safety incident log.

Sensitive or personal information will only be shared via email in accordance with data protection legislation.

2.4 Official videoconferencing and webcam use

All videoconferencing equipment in the classroom will be switched off when not in use and where appropriate, not set to auto answer.

Users

Pupils will ask permission from a teacher before making or answering a videoconference call or message.

Videoconferencing will be supervised appropriately for the pupils' age and ability.

Parents and carers consent will be obtained prior to children taking part in videoconferences.

Video conferencing will take place via official and approved communication channels following a robust risk assessment.

2.5 Appropriate and safe classroom use of the internet and associated devices

The school's internet access will be designed to enhance and extend education.

Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.

Pupils will use age and ability appropriate tools to search the Internet for content.

Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum.

The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.

All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.

Supervision of pupils will be appropriate to their age and ability

At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.

All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.

3. Social Media Policy

3.1. General social media use

Expectations regarding safe and responsible use of social media will apply to all members of Patcham Junior School community and exist in order to safeguard both the school and the wider community, on and offline. Please refer to the Social Media Policy for more detailed information.

Examples of social media may include blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, apps, video/photo sharing sites, chatrooms, instant messenger and many others.

All members of Patcham Junior School community will be encouraged to engage in social media in a positive, safe and responsible manner at all times.

Information about safe and responsible use of social media will be communicated clearly and regularly to all members of Patcham Junior School community.

All members of Patcham Junior School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

The use of social networking applications during school hours for personal use is/is not permitted.

Inappropriate or excessive use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of Internet facilities

Any concerns regarding the online conduct of any member of Patcham Junior School community on social media sites should be reported to the school leadership team and will be managed in accordance with existing school policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with the relevant school policies, such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.

3.2. Staff official use of social media

If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and that they are an ambassador for the school.

Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the school.

Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.

Staff using social media officially will always act within the legal frameworks they would adhere to within school, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.

Staff must ensure that any image posted on the school social media channel have appropriate written parental consent.

Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.

Staff using social media officially will inform their line manager, the school online safety (e-Safety) lead and/or the head teacher of any concerns such as criticism or inappropriate content posted online.

Staff will not engage with any direct or private messaging with pupils or parents/carers through social media and should communicate via school communication channels.

Staff using social media officially will sign the school social media Acceptable Use Policy before official social media use will take place.

3.3 Staff personal use of social media

Personal use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Acceptable Use Policy.

All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this will be discussed with line manager/ member of Leadership Team/Headteacher.

If ongoing contact with pupils is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.

All communication between staff and members of the school community on school business will take place via official approved communication channels (such as school email address or phone numbers). Staff must not use personal accounts or information to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher/manager.

Any communication from pupils/parents received on personal social media accounts will be reported to the schools designated safeguarding lead.

Information staff members have access to as part of their employment, including photos and personal information about pupils and their family members, colleagues etc. will not be shared or discussed on personal social media sites.

All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and should ensure that their social media use is compatible with their professional role, in accordance with schools policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.

Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.

Members of staff will notify the Leadership/Management Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.

3.4 Pupils use of social media

Safe and responsible use of social media sites will be outlined for pupils and their parents as part of the school Acceptable Use Policy.

Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.

Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.

Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.

Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.

Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.

Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.

Any official social media activity involving pupils will be moderated by the school where possible.

The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the School will not create accounts within school specifically for children under this age.

Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members Patcham Junior School community to take steps to ensure that mobile phones and personal devices are used responsibly.

The use of mobile phones and other personal devices by young people and adults will be decided by the school and covered in appropriate policies including the school Acceptable Use or Mobile Phone Policy.

Patcham Junior School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers but requires that such technologies need to be used safely and appropriately within school.

4.2 Expectations for safe use of personal devices and mobile phones

Electronic devices of all kinds that are brought in to school are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.

Members of staff will be issued with a school/work phone number and email address where contact with pupils or parents/carers is required.

All members of Patcham Junior School community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.

All members of Patcham Junior School community will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.

4.3. Staff use of personal devices and mobile phones

Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-exiting relationships which could compromise this must be discussed with leaders/managers. Exceptions might include where staff members are also parents of children within the school.

Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.

Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.

4.4. Visitors use of personal devices and mobile phones

Parents/carers and visitors must use mobile phones and personal devices in accordance with the schools policy.

Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.

5. Policy Decisions

5.1. Reducing online risks

Patcham Junior School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.

Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.

The school will ensure that appropriate filtering systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. Schools should include appropriate details about the systems in place.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer or device.

The school will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.

5.2. Authorising internet access

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

All staff, pupils and visitors will read and sign the School Acceptable Use Policy before using any school ICT resources.

Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.

Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.

When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

6. Engagement Approaches

6.1 Engagement and education of children and young people

An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.

Education about safe and responsible use will precede internet access.

Pupils input will be sought when writing and developing school online safety policies and practices.

Pupils will be supported in reading and understanding the school Acceptable Use Policy in a way which suits their age and ability.

All users will be informed that network and Internet use will be monitored.

6.2 Engagement and education of children and young people who are considered to be vulnerable

Patcham Junior School is aware that some children may be considered to be more vulnerable online due to a range of factors and will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENCO).

6.3 Engagement and education of staff

The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of school safeguarding practice.

To protect all staff and pupils, the school will implement Acceptable Use Policies which highlights appropriate online conduct and communication.

Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.

6.4 Engagement and education of parents and carers

Patcham Junior School recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.

Parents' attention will be drawn to the school online safety (e-Safety) policy and expectations in newsletters, letters, the school prospectus and on the school website.

A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well attended events e.g. parent evenings, transition events, fetes and sports days.

7. Managing Information Systems

7.1 Managing personal data online

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Full information regarding the schools approach to data protection and information governance can be found in the schools information security policy.

7.2 Security and Management of Information Systems

The security of the school information systems and users will be reviewed regularly.

Virus protection will be updated regularly.

Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.

7.3 Filtering Decisions

The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.

The school will ensure that age and ability appropriate filtering is in place whilst using school devices and systems to try and prevent staff and pupils from being accidentally or deliberately exposed to unsuitable content.

The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of.

If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated as appropriate.

Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.

All changes to the school filtering policy will be logged and recorded.

The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.

Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Police or CEOP immediately.

7.4 Management of applications (apps) used to record children's progress

The headteacher is ultimately responsible for the security of any data or images held of children.

Apps/systems which store personal data will be risk assessed prior to use.

Personal staff mobile phones or devices will not be used for any apps which record and store children's personal details, attainment or photographs.

Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs.

Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.

Staff and parents/carers will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

8. Responding to Online Incidents and Concerns

All members of the school/setting community will be informed about the procedure for reporting online safety (e-Safety) concerns (such as breaches of filtering, cyberbullying, illegal content etc.).

The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.

The Designated Safeguarding Lead (DSL) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the LEA Safeguarding Children Board thresholds and procedures.

Complaints about Internet misuse will be dealt with under the School's complaints procedure.

Complaints about online bullying will be dealt with under the School's anti-bullying policy and procedure

Any complaint about staff misuse will be referred to the head teacher

Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).

Pupils, parents and staff will be informed of the schools complaints procedure.

Staff will be informed of the complaints and whistleblowing procedure.

All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

The school will manage online safety (e-Safety) incidents in accordance with the school discipline/behaviour policy where appropriate.

The school will inform parents/carers of any incidents of concerns as and when required.

After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.

Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Safeguards Team or Police via 999 if there is immediate danger or risk of harm.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the Police.

If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.

If an incident of concern needs to be passed beyond the school then the concern will be escalated to the Education Safeguarding Team to communicate to other schools/settings in the LEA.

Parents and children will need to work in partnership with the school to resolve issues.

Appendix 1

9.1 Responding to concerns regarding Self-Generated Indecent Images of Children (SGIIOC or "Sexting")

Patcham Junior School ensure that all members of the community are made aware of the social, psychological and criminal consequences of sharing, possessing and creating incident images of children (known as "sexting").

The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.

Patcham Junior School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

If the school are made aware of incident involving indecent images of a child the school will:

- Act in accordance with the schools child protection and safeguarding policy and the relevant LEA Safeguarding Child Boards procedures.
- Immediately notify the designated safeguarding lead.
- Store the device securely.
- Carry out a risk assessment in relation to the children(s) involved.
- Consider the vulnerabilities of children(s) involved (including carrying out relevant checks with other agencies)
- Make a referral to children's social care and/or the police (as needed/appropriate).
- Put the necessary safeguards in place for children e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Implement appropriate sanctions in accordance with the schools behaviour policy but taking care not to further traumatise victims where possible.
- Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.

The school will not view the image unless there is a clear need or reason to do so.

The school will not send, share or save indecent images of children and will not allow or request children to do so.

If an indecent image has been taken or shared on the school/settings network or devices then the school will take action to block access to all users and isolate the image.

The school will need to involve or consult the police if images are considered to be illegal.

The school will take action regarding indecent images, regardless of the use of school/setting equipment or personal equipment, both on and off the premises.

The school will follow the guidance (including the decision making flow chart and risk assessment template) as set out in "'Sexting' in schools: advice and support around self-generated images. What to do and how to handle it".

The school will ensure that all members of the community are aware of sources of support.

9.2. Responding to concerns regarding Online Child Sexual Abuse

Patcham Junior School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns.

The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers.

Patcham Junior School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.

If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Police.

If the school are made aware of incident involving online child sexual abuse of a child then the school will:

- Act in accordance with the schools child protection and safeguarding policy and the relevant LEA Safeguarding Child Boards procedures.
- Immediately notify the designated safeguarding lead.
- Store any devices involved securely.
- Immediately inform the police via 101 (using 999 if a child is at immediate risk) or alternatively to CEOP by using the Click CEOP report form: http://www.ceop.police.uk/safety-centre/
- Where appropriate the school will involve and empower children to report concerns regarding online child sexual abuse
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Make a referral to children's social care (if needed/appropriate).
- Put the necessary safeguards in place for pupil(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
- Inform parents/carers about the incident and how it is being managed.
- Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.

9.3. Responding to concerns regarding Indecent Images of Children (IIOC)

Patcham Junior School will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.

The school will take action regarding of Indecent Images of Children (IIOC) regardless of the use of school/setting equipment or personal equipment, both on and off the premises.

The school will take action to prevent access accidental access to of Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.

If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Police.

9.4. Responding to concerns regarding radicalisation or extremism online

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils. Schools will need to highlight specifically how internet use will be monitored either here or within subsequent sections.

When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the school safeguarding policy.

9.5. Responding to concerns regarding cyberbullying

Cyberbullying, along with all other forms of bullying, of any member of Patcham Junior School community will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.

All incidents of online bullying reported will be recorded.

There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.

If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Sussex Police.

Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.

Appendix 2

Patcham Junior School Staff and Governors Acceptable Use Policy

School networked resources, including SIMS, are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. If you make a comment about the school or LEA you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the school or LEA into disrepute is not allowed.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access; monitoring and / or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

CONDITIONS OF USE

Personal Responsibility

Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to Designated Safeguarding Lead.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion. Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the school ethos and code of conduct.

1	I wil not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school (or LEA) into disrepute.
2	I will use appropriate language – I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden
3	I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4	I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.
5	Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person (see 21). I will not reveal any of my personal information to students.
6	I will not trespass into other users' files or folders.
7	I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users.
8	I will ensure that if I think someone has learned my password then I will change it immediately and/or contact DSL
9	I will ensure that I log off after my network session has finished.

10	If I find an unattended machine logged on under other users username I will not continue to use my machine – I will log it off immediately.
11	I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the school leadership team.
12	I am aware that e-mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
13	I will not use the network in any way that would disrupt use of the network by others.
14	I will report any accidental access, receipt of inappropriate materials or filtering breaches/unsuitable websites to the Designated Safeguarding Lead
15	I will not use personal USB drives, portable hard-drives, tablets or personal laptops on the network. I will only use my encrypted memory stick provided by the school.
16	I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
17	I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.
18	I will not accept invitations from children and young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine. As damage to professional reputations can inadvertently be caused by quite innocent postings or images – I will also be careful with who has access to my pages through friends and friends of friends. Especially with those connected with my professional duties, such as school parents and their children.
19	I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to, are not confused with my professional role in any way.
20	I will support and promote the school's e-safety and Data Security policies and help pupils be safe and responsible in their use of the Internet and related technologies.
21	I will not send or publish material that violates Data Protection Act or breaching the security this act requires for personal data, including data held in SIMS.
22	I will not receive, send or publish material that violates copyright law. This includes materials sent/received using Video Conferencing or Web Broadcasting.
23	I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.
24	I will ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used.
25	I will ensure that any Personal Data (where the Data Protection Act applies) that is sent over the Internet (or taken offsite in ay other way) will be encrypted or otherwise secured.

Appendix 3

Patcham Junior School

Rules for Responsible Computer Use

The school has computers and laptops with Internet access to help your learning. These rules will keep you safe and help us be fair to others.

- I will only access the system with my own login and password.
- I will not access other people's files or try to log on using anyone else's password;
- I will use the computers for school work during lesson time;
- I will not bring in memory sticks or discs from outside school unless I have been given permission and they have been checked by a member of staff for viruses;
- I will ask permission from a member of staff before using the Internet;
- I will only E-mail people I know, or my teacher has approved;
- The messages I send will be polite and responsible;
- I will not give my home address or telephone number, nor arrange to meet someone, unless my parent, carer or teacher has given permission;
- I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself;
- I understand that the school may check my computer files, may monitor the Internet sites I visit and may check my E-mails; I will use the Internet responsibly.
- I understand I may be monitored while using a computer in school and the teachers can see what I am doing at any time.

Appendix 3a

Dear Parents/Carers

Responsible Use of Computers and Internet

As your child progresses through the school, they will have increased access to the Internet, have their own school email address and have access to our new Learning Platform.

Please could you take some time to read through and discuss the 'Rules for Responsible Computer Use' with your child before both a parent and child sign the form and return it to the class teacher.

We take e-safety very seriously and are mindful of the problems there are with children gaining access to undesirable materials. We have taken steps, along with the Local Education Authority, to deal with this. Our Internet access is supplied by Brighton & Hove City Council and it has a highly effective, built in filtering system that restricts access to sites containing inappropriate content. All our screens are in public view and normally an adult is present to supervise. No system is perfect, however, and you should be aware that it is not possible to remove entirely the risk of finding unsuitable material.

If you have any further questions please contact me or email office@patchamjun.brighton-hove.sch.uk

Ashley Seymour-Williams
Headteacher

……

Child's Name…….. Class…….

By signing this we agree to the Rules of Responsible Computer Use

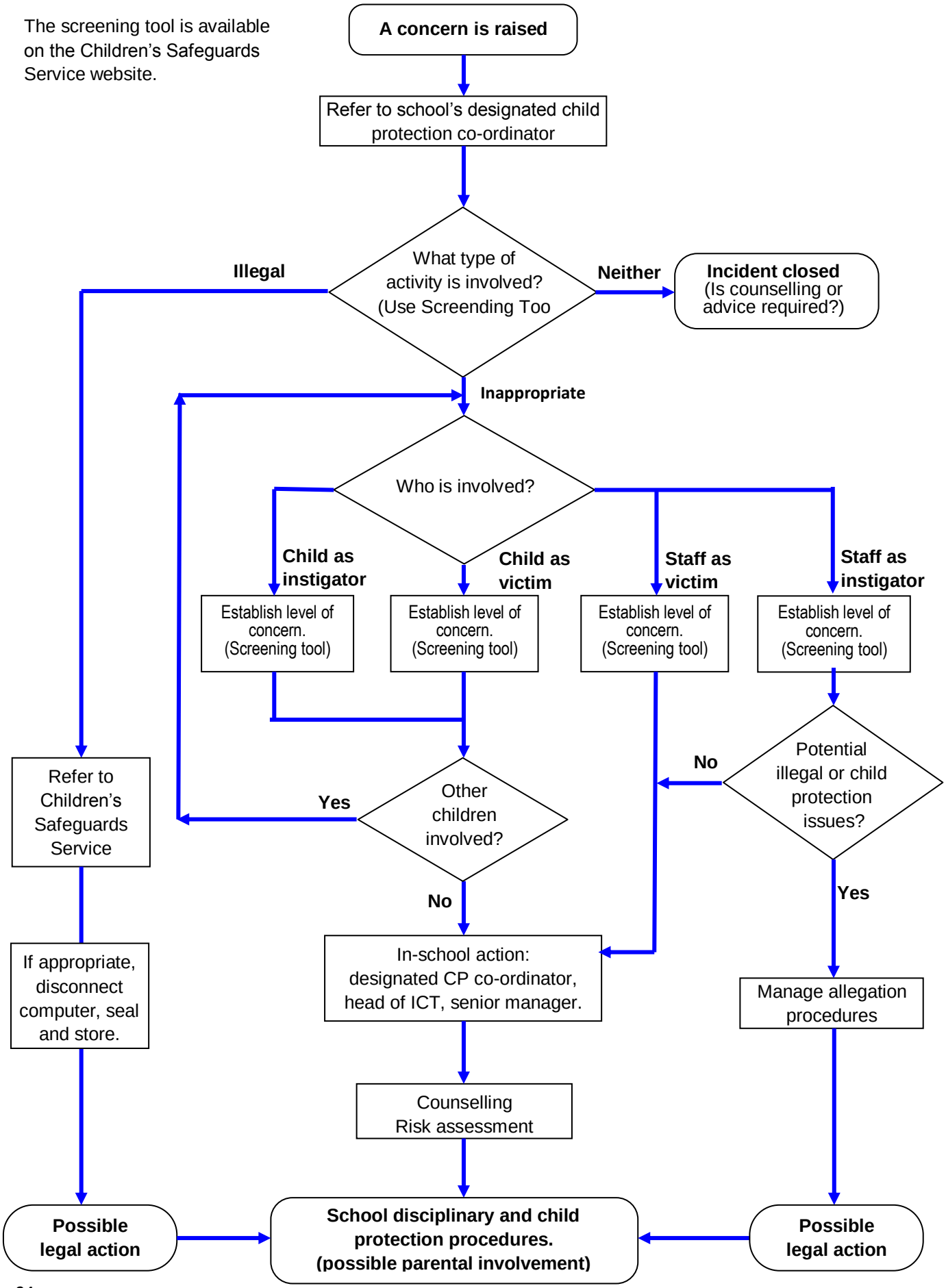
Signed by Child……

Signed by Parent……

Appendix 4

Response to an Incident of Concern

The screening tool is available on the Children's Safeguards Service website.



Appendix 5

Ladies Mile Road, Patcham, Brighton, East Sussex BN1 8TA
Telephone: 01273 295020

Dear Parents and Carers,

Children at Patcham Junior School should not need to bring mobile phones to school. The school advises all parents to discourage pupils from doing so as they are valuable and may be lost or stolen. They also can lead to pupils being distracted, bullying or children feeling left out.

We do also understand that for older children, particularly in year 6, there may be on occasion a legitimate reason for having a phone *after school* (e.g. if they walk a significant distance home alone)

If so, then please can you write a letter to me explaining why your child needs a phone. The letter will need to be countersigned by your child's teacher, giving permission for your child to have a phone in school.

Mobile phones that are unauthorised will be confiscated and **only returned to the parent, guardian or carer**. Similarly if mobiles are used on the school premises, during the school day for any purpose they will be confiscated. Following a letter of permission the following strict conditions apply:

- The letter, signed by both the parent and the headteacher is kept with the phone at all times.
- The phone is switched off and kept in the child's bag – never in the classroom.
- **The school accepts no liability for the loss/damage of any personal equipment whilst on school premises.**
- The phone is never used during the school day.
- The camera on the phone is never used by a child to take photographs or video of another child at school.
- If a pupil is found taking photographs or video footage with a mobile phone of either other pupils or teachers, this will be regarded as a serious offence and disciplinary action will be taken
- If images of other pupils or teachers have been taken at school, the phone will not be returned to the pupil until the images have been removed by the pupil in the presence of a teacher. The child's parents will be contacted and asked to discuss the matter with the Headteacher

Should parents/carers need to contact pupils in an emergency, or vice versa, this should be always be done following the usual school procedures: via the school office, Tel no 01273 295020

Thank you for supporting us in this matter.

Ashley Seymour-Williams

Staff User Agreement Form for the Staff Acceptable Use Policy

As a school user of the network resources, I agree to follow the school rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult <responsible officer>.

I agree to report any misuse of the network to the Designated Safeguarding Lead

I also agree to report any websites that are available on the school Internet that contain inappropriate material to Designated Safeguarding Lead.

Lastly I agree to ensure that portable equipment such as cameras or laptops will be kept secured when not in use and to report any lapses in physical security to Designated Safeguarding Lead.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Staff Name: _____

Staff Signature (if appropriate): _____

Date _____