# Furze Platt Junior School Online Safety Policy

<table>
<thead>
<tr>
<th>Document Version</th>
<th>1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason for Issue</td>
<td>Statutory</td>
</tr>
<tr>
<td>Document Author</td>
<td>Mike Wallace</td>
</tr>
<tr>
<td>Creation Date</td>
<td>Feb 2018</td>
</tr>
<tr>
<td>Approved by</td>
<td>Governing Body</td>
</tr>
<tr>
<td>Approval date</td>
<td>March 2018</td>
</tr>
<tr>
<td>Review frequency</td>
<td>In response to legislation Monitor implementation annually – T&amp;L committee</td>
</tr>
<tr>
<td>Document location</td>
<td>FPJS, Governor Policy Folder, Website</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Versio n</th>
<th>Date</th>
<th>Author</th>
<th>Status (Draft, approved etc)</th>
<th>Version History (Creation, update, archive)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>March 2018</td>
<td>MW</td>
<td>Approved</td>
<td>Creation</td>
</tr>
</tbody>
</table>
STATEMENT OF INTENT

FPJS is committed to the use of computer technologies and recognise access to the internet as a valuable tool for learners of all ages. The internet is increasingly providing the focal point of educational content within the UK. However, FPJS recognises that computers and the internet do have the potential for inappropriate use and access to undesirable material and that we have a duty of care to protect our pupils.

We are clear that all pupils should use computer facilities, including the internet, as an essential part of the planned curriculum and as a natural part of the modern learning opportunities within our school. However, we expect staff to educate our pupils about E-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies in and beyond the context of the classroom.

INTRODUCTION

This Policy and guidance has used the policy templates and assistance issued and updated by the South West Grid for Learning Trust. The SWGfL is an educational trust with an international reputation in supporting schools with online safety and a commitment to provide educational establishments with safe, secure and reliable teaching & learning resources and services.

SWGfL is a founding member of UKCCIS (UK Council for Child Internet Safety). Additional information about its services for schools can be found on the SWGfL website – www.swgfl.org.uk

This policy is not a statement of prescribed policy content or style which is a devolved responsibility of the local governing body. It is however a reminder of the statutory and advisory content of any such policy.

OBJECTIVES

Our Online Safety Policy Guidance is based on the key principles under which our schools

- ensure pupils’ internet use and access is appropriate and controlled.
- preventing misuse of internet connected devices.
- ensuring pupils and parents/carers are educated on the risks carried with internet use and how to minimise and deal with those risks.
- providing students with knowledge and resources to make decisions to ensure their safety online
- ensuring procedures and access is effectively managed to minimise risks

SCOPE

This policy applies to all members of FPJS including staff, pupils, volunteers, parents /carers, visitors, and other users of our schools and sites.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other E-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the
searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated policies and will, where known, inform parents / carers of incidents of inappropriate E-safety behaviour that take place out of school.

- Governing Body
- Teaching Staff
- Headteacher
- Support staff
- All School Staff
- Pupils
- Central Office Staff
- Parents/carers
- Contractors/ Service Providers
- Users of the school site and buildings

**RELEVANT LEGISLATION**

It is recommended that legal advice is sought from SLT in the advent of an e safety issue or situation.

- Computer Misuse Act 1990
- Data Protection Act 1998
- Freedom of Information Act 2000
- Communications Act 2003
- Malicious Communications Act 1988
- Copyright, Designs and Patents Act 1988
- Telecommunications Act 1984
- Criminal Justice & Public Order Act 1994
- Racial and Religious Hatred Act 2006
- Protection from Harassment Act 1997
- Protection of Children Act 1978
- Sexual Offences Act 2003
- Public Order Act 1986
- Obscene Publications Act 1959 and 1964
- Human Rights Act 1998
- The Education and Inspections Act 2006
- The Education and Inspections Act 2011
- The Protection of Freedoms Act 2012
- The School Information Regulations 2012
- Serious Crime Act 2015

**RELATED POLICIES**

- Safeguarding & Child Protection Policy
- Equality Policy
- School Anti-Bullying Policy
- Data Protection Policy
- Social Media Policy

**GENERAL PRINCIPLES**

Definitions

- Unless indicated otherwise, all references to “teacher” include the Headteacher;
- Unless indicated otherwise, all references to ‘staff’ include teaching and support staff.
- The term E-Safety refers to all aspects of the taught and untaught curriculum and in the home, where children and young people communicate using electronic media, fixed and mobile devises
which have access to the internet. It focuses on ensuring that children and young people are protected from harm and supported to achieve the maximum benefit from new and developing technologies without risk to themselves or others.

**MONITORING & EVALUATION**

The Local Governing Body and Headteacher will monitor the operation and effectiveness of the school’s Online Safety Policy and deal with any queries relating to it or any concerns or complaints raised in relation to the policy on an annual basis.

**ROLES AND RESPONSIBILITIES**

**Governors:**
- Governors have devolved responsibility for the approval of their E-safety Policy and for reviewing the effectiveness of their policies.

This will be carried out by both Governors receiving regular information about E-safety incidents and monitoring reports.

**Headteacher and Senior Leaders:**

The Headteacher and senior leaders:
- have a duty of care for ensuring the safety (including E-safety) of all members of the school community.
- be aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff.
- ensure that the E-safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their E-safety roles and to train other colleagues, as relevant.
- ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-safety monitoring role.
- receive regular monitoring reports from the E-safety Co-ordinator.
- ensure that the managed service provider carries out the E-safety measures.

**E-safety Coordinator**

The Computing lead and the Headteacher are designated E-Safety Coordinators. They will:
- take day to day responsibility for E-safety issues and a leading role in establishing and reviewing the school E-safety policies.
- ensure that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place.
- provide training and advice for staff.
- liaise with external bodies.
- report on E-safety incidents to the Senior Leadership Team and keep a log of incidents to inform future E-safety developments.
- when applicable, review incident logs with Governors.

**Teaching and Support Staff**

FPJS staff should ensure:
they have an up to date awareness of E-safety matters and of the current school E-safety policy and practices
they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
they report any suspected misuse or problem to the E-Safety coordinators
all digital communications with pupils and parents / carers should be on a professional level and only carried out using official school systems
E-safety issues are embedded in all aspects of the curriculum and other activities
pupils understand and follow the E-safety and acceptable use policies
they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding lead (DSL)
The DSL is also trained in E-safety issues and is aware of the potential for serious child protection / safeguarding 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

Pupils:
FPJS is clear that pupils have a role to play in ensuring that their learning is supported by the safe and secure use of the internet, new technologies and mobile devices. to remain both safe and legal when using the internet, they will need to understand the appropriate behaviours and critical thinking skills and show they:

- are responsible for using the school digital technology systems in accordance with the school’s Acceptable Use Policy
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- know and understand policies on the use of mobile devices and digital cameras.
- know and understand policies on the taking/use of images and on cyber-bullying at an age appropriate level.
- understand the importance of adopting good E-safety practice when using digital technologies out of school and realise that the school’s E-safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers
FPJS believes that Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. FPJS expects parents and carers to be
encouraged to support the school in promoting good E-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children’s personal devices in the school and home; especially around device security and social media use.
Online Safety Policy Guidance

1. Pupils

1.1. The education of pupils in E-safety is an essential part of the school’s curriculum provision. FPJS believes children and young people need the help and support of our schools and a well-planned curriculum to recognise and avoid E-safety risks and build their resilience.

1.2. Pupils at FPJS will also be taught stand-alone E-Safety lessons on Safer internet Day and also through external consultant enrichment day (http://www.pclstraining.com/)

1.3. FPJS expects E-safety to be a focus in all areas of the curriculum and for all staff to reinforce E-safety messages across the curriculum. Governors are urged to ensure that the E-safety curriculum is broad, relevant and provides progression, with opportunities for creative activities:

- A planned E-safety curriculum as part of Computing/IT, PHSE and other lessons and should be regularly revisited
- Key E-safety messages reinforced as part of a planned programme of assemblies and tutorial and pastoral activities; focusing on SMART as a reminder to pupils
- Pupils taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils taught to respect copyright when using material accessed on the internet
- Pupils taught to respect copyright when using material accessed on the internet
- Pupils taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils taught to respect copyright when using material accessed on the internet
- Pupils helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff acting as good role models in their use of digital technologies, the internet and mobile devices
- Pupils guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Staff being vigilant in monitoring the content of the websites the young people visit.
- Where pupils research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be made to the Headteacher & E-Safety coordinator, with clear reasons for the need.

2. Parents / Carers

2.1. FPJS is clear that an understanding of E-safety risks and issues is not a reliable skill set for parents and carers but are clear that they play an essential role in the education of their children and in the regulation of the children’s on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. FPJS will support parents / carers understanding through:

- Letters, newsletters and web site
- Parents / Carers information sessions
- High profile events and campaigns e.g. Safer Internet Day
Reference to the relevant E-safety web sites / publications for example

3. Governors
3.1. FPJS expects its Governors to take part in E-safety training, with particular importance for those who are members of T&L or lead Governors for, E-safety, health and safety and child protection.

4. Technical – infrastructure equipment, filtering and monitoring
4.1. FPJS ensures that the managed service provider carries out all the E-safety measures that would otherwise be the responsibility of the school. The managed service provider must be fully aware of the trust’s and school’s E-safety Policy and the agreed Acceptable Use Agreements.
4.2. FPJS E-Safety coordinators must ensure that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved are implemented.
4.3. FPJS expects that teaching about the responsibilities of internet use to include an awareness that
- School technical staff regularly monitor and record the activity of users on the school technical systems
- A system is in place for users to report any technical incident or security breach to the relevant person.
- Security measures to protect the school’s system from accidental or malicious attempts to access the school’s systems and data.
- the extent of personal use that users and their family members are allowed on school devices
- the use of removable media (e.g. memory sticks) by users on school devices is not permitted
- the encryption or otherwise of secured and personal data.

5. Bring Your Own Device (BYOD)
5.1. FPJS is aware of the educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of E-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. All BYOD must be agreed first by the Headteacher.

6. Use of digital and video images
6.1. FPJS is aware that the development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded
themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may

- provide avenues for cyberbullying to take place
- remain available on the internet forever
- cause harm or embarrassment to individuals in the short or longer term.

6.2. FPJS curriculum includes teaching of risks and to the E-Safety coordinators implement policies to reduce the likelihood of the potential for harm:

6.3. When using digital images, staff will 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 on the internet.

6.4. FPJS recognises the guidance from the Information Commissioner’s Office on the taking of videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). FPJS is clear that any such images should not be published or made publicly available on social networking sites. Parents/carers will also be warned about making comment on any activities involving other pupils in the images.

7. Communication & Mobile Technology

7.1. Pupils are not permitted to bring mobile devices into school, unless agreed by the Headteacher (BYOD) or needed for safe access to and from school – in this occasion, devices must be handed to the class teacher for the duration of the school day. Any devices not handed in or used inside the school grounds, will be confiscated and handed to the Headteacher.

<table>
<thead>
<tr>
<th>Communication Technologies</th>
<th>Staff and other Adults</th>
<th>Students / Pupils</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile phones may be brought to school</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Use of mobile phones in lessons</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Use of mobile phones in social time</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Taking photos on mobile phones / cameras</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Use of other mobile devices e.g. tablets, gaming devices</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
8. Social Media - Protecting Professional Identity

8.1. Expectations for teachers’ professional conduct are set out in ‘Teachers Standards 2012’

8.2. All staff have a duty of care to provide a safe learning environment for pupils. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party, and/or may be subject to criminal and internal disciplinary procedures.

8.3. The staff conduct policy reinforces that:
   - No reference should be made in social media to pupils, parents/carers or other school staff
   - They do not engage in online discussion on personal matters relating to members of the school community
   - Personal opinions should not be attributed to the school

8.4. School’s use of social media for professional purposes will be checked regularly by the Headteacher.

9. Unsuitable / inappropriate activities

9.1. Certain types of internet activity e.g. accessing child abuse images, cyber bullying and distributing racist material is illegal and is therefore not permitted. Such action could lead to criminal prosecution.

9.2. In addition there are a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

9.3. FPJS believes that the activities referred to below, would be inappropriate in a school context or, in some cases risk disclosing personal passwords and bank details on open school systems and that users should not engage in these activities when using school equipment:
   - Using school systems to run a private business
   - Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy
   - Infringing copyright
   - Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
   - Creating or propagating computer viruses or other harmful files
- Unfair usage (downloading / uploading large files that hinders others in their use of the internet)
- On-line gaming (non-educational)
- On-line gambling
- On-line shopping/commerce
- File sharing
- Use of messaging apps

Responding to incidents of misuse

9.4. This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

9.5. If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart in Appendix D F for responding to online safety incidents and report immediately to the police.

Other Incidents

9.6. FPJS expects all members of the school community to be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

9.7. In the event of suspicion, FPJS expects its senior leaders and governors to act promptly and to take all the steps in this procedure:

- Have more than one senior member of staff and/or governor involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the investigation using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- Ensure during the investigation that the sites and content visited are closely monitored and recorded (to provide further protection); recording the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the record (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the individual will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement RBWM staff or national/local organisations (as relevant).
  - Police involvement and/or action

If the content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
- incidents of ‘grooming’ behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

9.8. It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form (see appendix C) should be retained by the investigating panel for evidence and reference purposes.

10. School Actions & Sanctions

10.1. It is more likely that our schools will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that pupils are aware of the standards in place to minimise any breaches. It is expected that incidents of misuse will be dealt with through normal behaviour policies and procedures.

- Deliberately accessing or trying to access material that could be considered illegal
- Unauthorised use of non-educational sites during lessons
- Unauthorised use of mobile phone, digital camera and/or other mobile device
- Unauthorised use of social media/messaging apps or personal email
- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords
- Attempting to access or accessing the school network, using another pupil’s account or the account of a member of staff
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
Appendices

Appendix A  Pupil Acceptable Use Agreement Form

I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of “stranger danger”, when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).

I will act as I expect others to act toward me:

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I may lose access to the school network, receive other sanctions and my teacher may contact my parents. In the event of illegal activities this may involve the police.

I have read and understand the above and agree to follow these guidelines when I use the school systems and devices (both in and out of school).

Name of Pupil:  

Group / Class:  

Signed:  

Date:
Appendix B

Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school 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 online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.
- that parents and carers keep up to date with the law regarding online social media use and how this can put their child’s safety at risk.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

The statements below must be agreed to by all parents and carers of FPJJS.

I agree that if I take digital or video images at, or of – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

I agree that I will monitor my child’s online use, regularly check History, apply safe security device locks and not permit my child to use age restricted sites, games or social media.

Parents are requested to adhere to these safety expectations.
Appendix C

Responding to incidents of misuse – flow chart

Online Safety Incident

- Unsuitable Materials
  - Report to the person responsible for Online Safety
  - If staff/Volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
  - Debrief on online safety incident
  - Review policies and share experience and practice as required
  - Implement changes
  - Monitor situation

- Illegal materials or activities found or suspected
  - Illegal Activity or Content (No immediate risk)
  - Illegal Activity or Content (Child at Immediate Risk)
  - Staff/Volunteer or other adult
    - Report to CEOP
    - Call professional strategy meeting

- Illegal Activity or Content (No immediate risk)
  - Secure and preserve evidence
  - Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
  - If no illegal activity or material is confirmed then revert to internal procedures
  - In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action
Appendix D

Responding to incidents of misuse – record form

Group: .....................................................................................................................

Date: .......................................................................................................................

Reason for investigation: ............................................................................................
........................................................................................................................................
........................................................................................................................................

Details of first reviewing person

Name: ......................................................................................................................

Position: ...................................................................................................................

Signature: ...................................................................................................................

Details of second reviewing person

Name: ......................................................................................................................

Position: ...................................................................................................................

Signature: ...................................................................................................................

Name and location of computer used for review (for web sites)
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................

<table>
<thead>
<tr>
<th>Web site(s) address / device</th>
<th>Reason for concern</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Reporting Log

**Group:** .......................................................... 

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Incident</th>
<th>Action Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>What?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>By Whom?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Incident</th>
<th>Action Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Incident</th>
<th>Action Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Conclusion and Action proposed or taken**

- 
- 
- 
- 
- 
- 
- 


Links to other organisations or documents

The following links may help those who are developing or reviewing school online safety policies:

- UK Safer Internet Centre
- Safer Internet Centre – [http://saferinternet.org.uk/](http://saferinternet.org.uk/)
- Professionals Online Safety Helpline - [http://www.saferinternet.org.uk/about/helpline](http://www.saferinternet.org.uk/about/helpline)
- Internet Watch Foundation - [https://www.iwf.org.uk/](https://www.iwf.org.uk/)
- CEOP
- CEOP - [http://ceop.police.uk/](http://ceop.police.uk/)
- ThinkUKnow - [https://www.thinkuknow.co.uk/](https://www.thinkuknow.co.uk/)

Others

- UK Council for Child Internet Safety (UKCCIS) - [www.education.gov.uk/ukccis](http://www.education.gov.uk/ukccis)

Tools for Schools

- Online Safety BOOST – [https://boost.swgfl.org.uk/](https://boost.swgfl.org.uk/)

Bullying / Cyberbullying

- Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGFL & Diana Awards) - [http://enable.eun.org/](http://enable.eun.org/)
- Anti-Bullying Network – [http://www.antibullying.net/cyberbullying1.htm](http://www.antibullying.net/cyberbullying1.htm)

Social Networking

- Digizen – [Social Networking](http://www.digizen.co.uk)
- UKSIC - [Safety Features on Social Networks](http://www.englishpartnerships.org.uk/practices/safetyfeatures)
- SWGFL - Facebook - Managing risk for staff and volunteers working with children and young people
- Connectsafely Parents Guide to Facebook
- Facebook Guide for Educators

Curriculum

- [SWGFL Digital Literacy & Citizenship curriculum](http://www.swgfl.org.uk/curriculum/)
- Teach Today – [www.teachtoday.eu/](http://www.teachtoday.eu/)
- Insafe - [Education Resources](http://www.insafe.net/)
- Mobile Devices / BYOD
- Cloudlearn Report [Effective practice for schools moving to end locking and blocking](http://www.cloudlearn.org.uk/)
- NEN - [Guidance Note - BYOD](http://www.cloudlearn.org.uk/)
Data Protection

Information Commissioners Office:

- Your rights to your information – Resources for Schools - ICO
- Guide to Data Protection Act - Information Commissioners Office
- Guide to the Freedom of Information Act - Information Commissioners Office
- ICO guidance on the Freedom of Information Model Publication Scheme
- ICO Freedom of Information Model Publication Scheme Template for schools (England)
- ICO - Guidance we gave to schools - September 2012 (England)
- ICO Guidance on Bring Your Own Device
- ICO Guidance on Cloud Hosted Services
- Information Commissioners Office good practice note on taking photos in schools
- ICO Guidance Data Protection Practical Guide to IT Security
- ICO – Think Privacy Toolkit
- ICO – Personal Information Online – Code of Practice
- ICO Subject Access Code of Practice
- ICO – Guidance on Data Security Breach Management
- SWGfL - Guidance for Schools on Cloud Hosted Services
- LGfL - Data Handling Compliance Check List
- NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training

- DfE - Safer Working Practice for Adults who Work with Children and Young People
- Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs
- Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
- UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

- NEN - Guidance Note - esecurity

Working with parents and carers

- SWGfL Digital Literacy & Citizenship curriculum
- Online Safety BOOST Presentations - parent’s presentation
- Connectsafely Parents Guide to Facebook
- Vodafone Digital Parents Magazine
- Childnet Webpages for Parents & Carers
- Get Safe Online - resources for parents
- Teach Today - resources for parents workshops / education
- The Digital Universe of Your Children - animated videos for parents (Insafe)
- Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
- Insafe - A guide for parents - education and the new media
- The Cybersmile Foundation (cyberbullying) - advice for parents

Research

- Futurelab - "Digital participation - its not chalk and talk any more!"
- Ofcom – Children & Parents – media use and attitudes report - 2015