**Linton Primary School,** Linton, Morpeth, Northumberland, NE61 5SG
Tel\Fax: 01670 860361
e-mail: admin@linton.northumberland.sch.uk
website: www.linton.northumberland.sch.uk

# E-SAFETY POLICY 2016

This policy was adapted by the Governing Body in the Summer Term of 2016 and will next be reviewed in the Summer Term 2017.

This policy applies to all members of the school - including staff, pupils, volunteers, parents / carers, visitors and community users who have access to and are users of school ICT systems, both in and out of the school.

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 (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by our Behaviour Policy.

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

## Roles and Responsibilities

### Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Curriculum Committee and the Child Protection Governor, Michael Watson, who receives an annual report within the Child Protection report.
Governor training will be given as appropriate – usually this will be to the Curriculum Committee.

### Headteacher

The Headteacher is the E-Safety lead and is also the Designated Teacher for Child Protection and has a duty of care for ensuring the safety of members of the school community.

The Headteacher is aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff or an E-Safety incident. A flow chart is attached to the appendix.

The Headteacher has undertaken CEOPS training on 4.10.13 and 20.1.16. The role has the following responsibilities:

- Day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Discusses e-safety with the Governing Body through committee meetings, Headteacher reports to the Governors and an annual meeting with the Child Protection Governor
- Ensures that the curriculum informs children about e-safety, including sharing personal data, inappropriate on-line contact with adults or strangers, cyber-bullying, accessing inappropriate content and grooming

- Ensures that the school IT system is protected by filtering and monitoring software, has appropriate protection. The Headteacher monitors reports through Policy Central Enterprise on a weekly basis.

## School IT System

The school will make sure that the IT system supports E-Safety and is as safe as possible. By purchase of appropriate SLAs, equipment and software, we will ensure that:

- The school's  technical infrastructure is secure and is not open to misuse or malicious attack
- The school meets required  e-safety technical requirements and any Local Authority E-Safety guidance that may apply.
- Users may only access the admin networks through a properly enforced password protection policy, in which passwords are regularly changed
- Filtering software, is applied and updated on a regular basis
- We keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- The use of the internet and NORTLE is regularly monitored in order that any misuse  can be investigated
- That monitoring software is in place and regularly updated
- Wireless systems are password protected and access is not given unless approved by the Headteacher
- Admin and Network Passwords are kept securely and locked away
- Pupils have access to their own log in password for Schools 360 and online software

## Teaching and Support Staff

Staff are responsible for ensuring that 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 (AUP)
- they report any suspected misuse or problem to the Headteacher  for investigation
- ensure that all digital communications with pupils / 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

Any use of school mobile devices off school premises is applicable to our AUP. Staff should sign out any equipment taken home. Use on devices on home internet is discouraged. Monitoring software is still applicable at home and staff should be aware that use is monitored and checked on a weekly basis by the Headteacher.

## Designated Person for Child Protection

The Designated Person should be trained in e-safety issues and be 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

It is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop

## Pupils:

Pupils are responsible for using the school digital technology systems in accordance with the Acceptable Use Policy

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be aware of using technology safely and in acceptable boundaries
- should 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

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. The school  will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, NORTLE and information about e-safety events and campaigns.

Parents and carers will 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
- access to the website, Schools 360 and on-line software
- children do not bring personal devices to school

## Community Users

Community users do not currently have access to the school's ICT equipment. They are informed on first contact with the school that mobile devices should be switched off in the presence of pupils.

## Our Curriculum

Pupils will be taught to take a responsible approach to using technology and our curriculum is an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum.

The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of  Computing lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided by staff to the accuracy of information.
- Pupils should be 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 should act as good role models in their use of digital technologies  the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. A firewall is in place through LA network.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the LA ICT Team can temporarily remove those sites from the filtered list  for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

## Use of digital and video images

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. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take 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). To respect everyone’s privacy and in some cases protection, these images should not be published on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers  are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those  images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website this is covered as part of the AUA signed by parents or carers at the start of the year
- Pupil’s work can only be published with the permission of the pupil and parents or carers.

## Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject’s rights

- Secure
- Only transferred to others with adequate protection.

Following a number of “high profile” losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.

The school  must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- The Headteacher is identified as the Responsible persons
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- A policy about the use of cloud storage / cloud computing will be developed if necessary which ensure that such data storage meets the requirements laid down by the Information Commissioner’s Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices. School has provided each member of staff with an encrypted memory stick and this is the only device to be used on school machines.

When  personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many  memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

## Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using  these technologies for education outweighs their  risks / disadvantages

| | **Staff and Other Adults** | | | | **Pupils** | | | |
|---|---|---|---|---|---|---|---|---|
| **Communication Technologies** | Not allowed | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission |
| Mobile phones may be brought to school | | ▯ | | | ▯ | | | |
| Use of mobile phones in lessons | ▯ | | | | | | | |
| Use of mobile phones in social time | | ▯ | | | | | | |
| Taking photos on mobile phones / cameras | ▯ | | | | | | | |
| Use of other mobile devices eg tablets, gaming devices | School has a set of ipads which are used by staff and children during school. | | | | | | | |
| Use of personal email addresses in school, or on school network | ▯ | | | | ▯ | | | |
| Use of school email for personal emails | ▯ | | | | ▯ | | | |
| Use of messaging apps | Messaging apps have been disabled on ipads | | | | | | | |
| Use of social media | | | ▯ | | ▯ | | | |
| Use of blogs | ▯ | | | | | | | |

When using communication technologies the school considers the following as good practice:

- The official school  email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.  Staff should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).

- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and pupils or parents / carers (email, chat, Schools 360 etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils will send e-mails through the school admin system and will be assisted by the Admin Officer to do so.

- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

## Social Media - Protecting Professional Identity

We have adopted NCC Code of Conduct which details Social Media Use and with an increase in use of all types of social media for professional and personal purposes this policy should be followed as is sets out clear guidance for staff to manage risk and behaviour online.

This is paramount for the protection of pupils, the school and the individual when publishing any material online.

Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. While, Ofsted's e-safety framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment.

Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or 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 or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school currently does not use social media for professional purposes.

## Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems.

Other activities eg cyber-bullying would be banned and could lead to criminal prosecution.

There are however 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.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

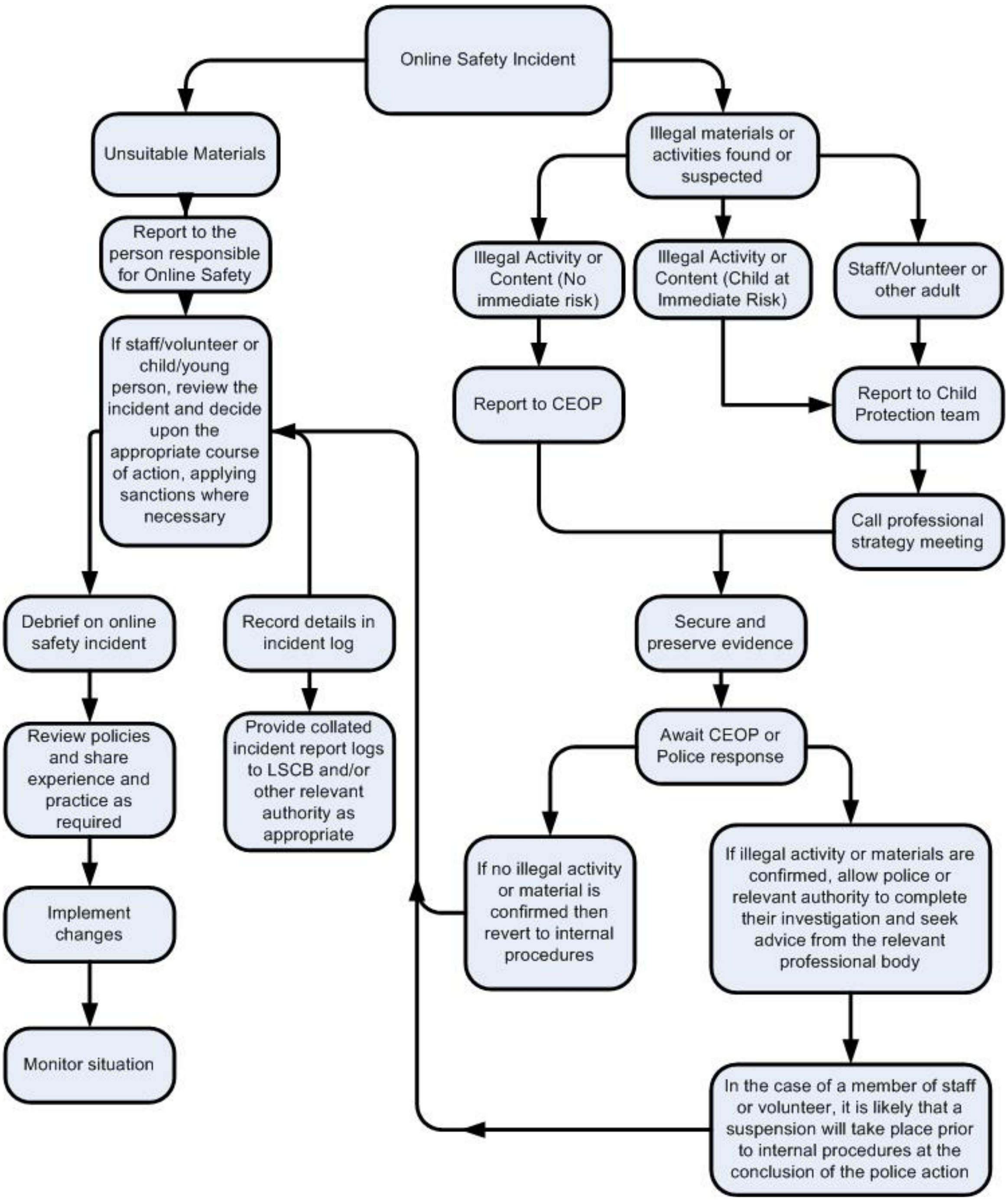
| **User Actions** | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| **Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:** | **Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978** | | | | | X |
| | **Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.** | | | | | X |
| | **Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008** | | | | | X |
| | **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986** | | | | | X |
| | **pornography** | | | | X | |
| | **promotion of any kind of discrimination** | | | | X | |
| | **threatening behaviour, including promotion of physical violence or mental harm** | | | | X | |
| | **any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute** | | | | X | |
| **Using school systems to run a private business** | | | | | X | |
| **Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy** | | | | | X | |
| **Infringing copyright** | | | | | X | |
| **Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)** | | | | | X | |
| **Creating or propagating computer viruses or other harmful files** | | | | | X | |
| **Unfair usage (downloading / uploading large files that hinders others in their use of the internet)** | | | | | X | |
| **On-line gaming (educational)** | | | | | X | |
| **On-line gaming (non educational)** | | | | | X | |
| **On-line gambling** | | | | | X | |
| **On-line shopping** | | | | X | | |
| **File sharing** | | | | X | | |
| **Use of social media** | | | X | | | |
| **Use of messaging apps** | | | | | X | |
| **Use of video broadcasting eg Youtube** | | | | | X | |

## Responding to incidents of misuse

NCC Guidance should be followed for managing incidents – a copy is placed next to each set of IT equipment to assist staff.

### Illegal Incidents

**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 (below and appendix) for responding to online safety incidents and report immediately to the police.**


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
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
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
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

## Other Incidents

It is hoped that all members of the school community will 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.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one person involved in this process. This is vital to protect individuals if accusations are subsequently reported. In our case this will be the Headteacher and the Child Protection Governor. Concerns will be reported to the NCC officer responsible for E-Safety incidents.

- Conduct the procedure 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.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also 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 form (except in the case of images of child sexual abuse – see below)

- Once this has been completed and fully investigated the group 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 by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action

- If 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.

It is important that all of 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 should be retained for evidence and reference purposes.

## School Actions and Sanctions

It is more likely that the school 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 members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour  or disciplinary procedures as follows:

### Pupils

| Incidents: | Refer to class teacher | Refer to Headteacher | Refer to Police | Refer to technical support  staff for action re filtering / security  etc | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction eg detention / exclusion |
|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | | X | X | | X | X | X | X |
| Unauthorised use of non-educational sites during lessons | | X | | | | | X | |
| Unauthorised use of mobile phone / digital camera / other mobile device | | X | | | | | X | |
| Unauthorised use of social media /  messaging apps / personal email | | X | | | | | | |
| Unauthorised downloading or uploading of files | X | X | | X | | | | |
| Allowing others to access school / academy network by sharing username and passwords | | X | | | X | | X | X |
| Attempting to access or accessing the school / academy network, using another student's  / pupil's account | X | X | | | X | | | |
| Attempting to access or accessing the school / academy network, using the account of a member of staff | | X | | | X | | X | X |
| Corrupting or destroying the data of other users | X | X | | X | X | X | X | X |
| Sending an email, text or  message that is regarded as offensive, harassment or of a bullying nature | | X | | | X | | X | X |
| Continued infringements of the above, following previous warnings or sanctions | | X | X | | X | | | X |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | | X | | | X | X | X | X |
| Using proxy sites or other means to subvert the school's / academy's filtering system | | X | | X | X | | | X |
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | X | | | X | | | |
| Deliberately accessing or trying to access offensive or pornographic material | | X | X | | X | | | X |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | | X | | | X | | X | X |

| **Staff** | **Actions** | | | | | | |
|---|---|---|---|---|---|---|---|
| Incidents: | Refer to Headteacher | Refer to Local Authority / HR | Refer to Police | Refer to Technical Support Staff for action re filtering etc | Warning | Suspension | Disciplinary action |
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | X | X | X | | | X | X |
| Inappropriate personal use of the internet / social media / personal email | X | X | | | X | | |
| Unauthorised downloading or uploading of files | X | | | X | | | |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account | X | | | X | X | | |
| Careless use of personal data eg holding or transferring data in an insecure manner | X | X | | | X | | X |
| Deliberate actions to breach data protection or network security rules | X | X | X | | | X | X |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | X | X | | | X | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | X | | X | | X |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils | X | X | | | X | | |
| Actions which could compromise the staff member's professional standing | X | | | | X | | X |
| Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy | X | X | | | X | X | X |
| Using proxy sites or other means to subvert the school's / academy's filtering system | X | X | | X | X | | X |
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | X | X | X | | | |
| Deliberately accessing or trying to access offensive or pornographic material | X | X | X | X | | X | X |
| Breaching copyright or licensing regulations | X | | | | X | | |
| Continued infringements of the above, following previous warnings or sanctions | X | X | | | | X | X |

## Monitoring and Review of this Policy

This e-safety policy has been developed by staff in consultation with parent Governors.

Consultation with the whole school community has taken place through the school website. The school will monitor the impact of the policy using logs of reported incidents, PCE reports, pupils survey.

**Summer 2016**