shortstay

Northumberland's P.R.U.

E-Safety Policy

All Staff (including Agency and Student Teachers), Parents / Carers, Volunteers and Management Committee

Approved by the Headteacher, Mr R Carr	**Date: 3rd August 2022**
Approved by the Governing Body	**Date: October 2022**
Last Reviewed On:	**Date: 3rd August 2022**
Next Review Due By:	**Date: 5th August 2023**

Northumberland
County Council

Introduction

At Northumberland PRU we take e-safety very seriously and see it as our duty to keep both our staff and pupils safe whilst using technology, not only in school, but also at home. This also includes our duty to keep our pupils safe from radicalisation and extremism (Prevent Duty).

As a professional organisation with responsibility for children's safeguarding, it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner.

To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign an Acceptable Use Policy. This clearly states the responsibilities of staff (including agency staff, student teachers, volunteers and governors) using technology in the work place. This will be signed when they commence their employment at Northumberland PRU and will be re-enforced each year during the staff's e-safety briefing and daily meetings where necessary.

This policy has been written in conjunction with the following key documents:

- Keeping Children Safe in Education (2016)
- 360 Degrees Safe website: https://360safe.org.uk/about-the-tool
- UK Safer Online Centre Website: http://www.saferinternet.org.uk/
- Child Exploitation and Online Safety Website: http://ceop.police.uk

1. Development / Monitoring / Review of this Policy

This e-safety policy has been developed by the Data and Progress Manager who also has responsibility for GDPR within school.

2. Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Northumberland PRU Management Committee on:	DRAFT
The implementation of this e-safety policy will be monitored by the:	Data and Progress Manager / Northumberland County Council IT Services Team / Senior Leadership Team
Monitoring will take place at regular intervals:	September 2022 and repeated every year
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	September 2022 and repeated every year
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Senior Leadership Team (SLT) – DSL (Designated Safeguarding Lead) / DpDSL (Deputy Designated Safeguarding Lead) Police

Northumberland PRU will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of pupils, parents / carers, staff

3. Scope of the Policy

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

3.2 The school will deal with such incidents within this policy along with associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of unsuitable e-safety behaviour that take place out of school. The response to incidents of unsuitable e-safety behaviour that take place in school will be in line with the school's Behaviour Policy. If an incident is more appropriate for child protection, such as in the form of peer to peer abuse; intervention will be in line with the Child Protection Policy.

4. Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

4.1 Management Committee

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 full Management Committee receiving regular information about e-safety incidents and monitoring reports. The

Management Committee will receive at least an annual update from the SLT team on incidents and any updates to the policy.

4.2 Headteacher and Senior Leaders

a. The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Data and Progress Manager, Sue Ingledew.
b. The Headteacher, DSL and DpDSL are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority disciplinary procedures as part of our Child Protection Policy).
c. The Headteacher is responsible for ensuring that the Data and Progress Manager, DSL and DpDSL receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
d. The Data and Progress Manager and Northumberland County Council IT Services Network Manager will 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 as recommended by Northumberland County Council Safeguarding team. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
e. The Senior Leadership Team will receive annual monitoring reports from the IT network team.
f. The Headteacher ensures training records are held which accurately record e-safety and safeguarding CPD for staff.

4.3 Data and Progress Manager – Sue Ingledew

As E-Safety lead, Sue Ingledew will:

a. take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies;
b. ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
c. provide training and advice for staff;
d. liaise with the Local Authority and regular external agencies;
e. liaise with Northumberland County Council IT Services team;
f. receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments – this log will be kept as part of the secure child protection logs;
g. meet with Governing Body when asked to discuss current issues, review incident logs and filtering / change control logs;
h. report regularly to Senior Leadership Team; and
i. be responsible for ensuring that all e-safety education is updated regularly and communicated with students through PSHCE, Computing lessons, assemblies and other areas of the curriculum.

The school will log any serious situation in the same way as any bullying or child protection incident via CPOMS.

4.4 Network Manager (Supplied by Northumberland County Council IT Services team):

The Network Manager is responsible for ensuring:

a. that the school's technical infrastructure is secure and is not open to misuse or malicious attack;
b. that the school meets required e-safety technical requirements and any Northumberland County Council ESafety Policy and Guidance that may apply;
c. that users may only access the networks and devices through a properly enforced password and Acceptable Use Policy;
d. the recommended Northumberland County Council filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person – but the Computing department needs to 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;
e. that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Data and Progress Manager/ DSL/ DpDSL or investigation / action / sanction; and
f. that monitoring software systems are implemented and updated as agreed in school.

4.5 Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

a. they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
b. they have read, understood and signed that they agree to the Staff Acceptable Use Policy (AUP);
c. they report any suspected misuse or problem to the Headteacher / Data and Progress Manager / DSL / DpDSL Officesr for investigation;
d. all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems which is the Northumberland PRU School Gmail account (firstname.lastname@pru.northumberland);
e. e-safety issues are embedded in all aspects of the curriculum and other activities;
f. pupils understand and follow the e-safety and Acceptable Use Policy;
g. pupils have a good understanding of research skills and the need to avoid plagiarism;
h. 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; and
i. 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.

4.6 DSL / DpDSL

The DSL and DpDSL should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

a. sharing of personal data;
b. access to illegal / unsuitable materials;
c. unsuitable on-line contact with adults / strangers;
d. potential or actual incidents of grooming;
e. cyber-bullying;

f. Prevent Strategy and Radicalisation; and
g. sexting

Any of the above issues may fall into either the Behaviour or Child Protection Policy and will be actioned as in line with the recommendations of these documents.

4.7 Pupils

a. are responsible for using the school digital technology systems and their own devices in accordance with the Pupil Acceptable Use Policy;
b. have a good understanding of research skills and the need to avoid plagiarism;
c. need to understand the importance of reporting abuse, misuse or access to unsuitable materials and know how to do so;
d. will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying; and
e. 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 could cover their actions out of school if it carries on into the school day. The school cannot be held responsible for student actions regarding internet use and social media outside of school hours.

4.8 Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through home partnership events, the Home School Agreement, the website and via the newsletter. 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:

a. digital and video images taken at school events;
b. access to parents' sections of the website and on-line pupil records; and
c. their children's personal devices in the school (where this is allowed).

4.9 Visitor Users

Visitor Users who access school systems / website as part of the wider school provision will be expected to sign the AUP (Acceptable Use Policy) before being provided with access to school systems.

5 Policy Statements

5.1 Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore 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. a planned e-safety curriculum should be provided as part of Computing / PSHCE / other lessons and should be regularly revisited;
b. key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities;
c. pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information;
d. pupils should be taught to acknowledge appropriate and relevant academic sources of information when accessing resources on the internet;
e. 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;
f. staff should act as good role models in their use of digital technologies the internet and mobile devices;
g. 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;
h. staff should be vigilant in monitoring the content of websites the pupils visit during lessons; and
i. it is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Data and Progress Manager 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 and reviewed by the Northumberland County Council IT Services team during the weekly meeting.

5.2 Education – Parents / Carers

Many parents have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and unsuitable material on the internet and may be unsure about how to respond.

The school will therefore seek to provide access to this policy and other guidance through the website and home partnership events.

6 Education & Training

6.1 Staff / Volunteers

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

a. a planned programme of formal e-safety training will be made available to staff as part of the annual Safeguarding update. This will be regularly updated and reinforced by the DSL, DpDSL and Data and Progress Manager at least annually;

b. all new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy;
c. the Data and Progress Manger and network manager (as supplied by Northumberland County Council IT Services) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations;
d. this E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days;
e. the Data and Progress Manager or network manager (as supplied by Northumberland County Council IT Services) will provide advice / guidance / training to individuals as required; and
f. the safe school guidelines offering advice to staff will be updated annually.

6.2 Training – Management Committee

The Management Committee should take part in e-safety training as part of the annual update to safeguarding children.

7 Technical – Infrastructure

7.1 Equipment, Filtering and Monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

a. school technical systems will be managed in real time in ways that ensure that the school meets recommended technical requirements outlined by Northumberland County Council;
b. there will be regular reviews and audits of the safety and security of school technical systems;
c. servers, wireless systems and cabling must be securely located and physical access restricted;
d. all users will have clearly defined access rights to school technical systems and devices;
e. all users (will be provided with a username and secure password by the Data and Progress Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password;
f. the Network Manager (as supplied by Northumberland County Council IT Services) must ensure passwords are secure but available to the Headteacher, DSL or DpDSL if required;
g. the Network Manager (as supplied by Northumberland County Council IT Services) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations;
h. internet access is filtered for all users as recommended by Northumberland County Council IT Services. The filtering system protects pupils without causing a negative impact on their education;

i. school staff regularly monitor and record the activity of users on the school systems and users are made aware of this in the Acceptable Use Policy. This is discussed and recorded where necessary;
j. an appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed. This involves referral to the Data and Progress Manager, DSL or DpDSL;
k. appropriate logical and physical security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from viruses, accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software;
l. an agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems. This involves signing the declaration on the Acceptable Use Policy for all staff;
m. an agreed Acceptable Use Policy is in place regarding the extent of personal use that users (staff / pupils / visitor users) and their family members are allowed on school devices that may be used out of school;
n. an agreed Acceptable Use Policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices;
o. an Acceptable Use Policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices.

7.2 Bring Your Own Device

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 regularly. 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.

a. The school has a set of clear expectations and responsibilities for all users as part of the Acceptable Use Agreement.
b. The school adheres to the General Data Protection Regulations (GDPR) principles.
c. All network systems are secure if pupils try to access the wi-fi on their own devices.
d. All users will use their username and password, and keep this safe, to access the school network.
e. Regular training is undertaken for staff.
f. Pupils receive guidance on the use of personal devices.
g. Regular monitoring of use will take place to ensure compliance.
h. Any device loss, theft, change of ownership of the device will not be the responsibility of the school.

Pupils are expected, when using their own devices, to adhere to the Acceptable Use Policy and Behaviour Policy of the school.

8 Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have taken / recorded themselves or downloaded from the internet. However, staff, parents 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. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

a. 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, on social networking sites;
b. 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 General Data Protection Regulations). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images;
c. staff are allowed to take digital / video images to support educational aims (where permission has been granted), but must follow school policies concerning the sharing, distribution and publication of those images. Pupils may request that they are not on anything that is published on line or in school. Digital images on staff devices should be transferred as soon as possible from their phones/tablets/personal computers to their school drive (user area) before being removed;
d. 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;
e. pupils must not take, use, share, publish or distribute images of others without their permission;
f. 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; and
g. the home school agreement allows pupils to opt out of their photograph and work being published on the school website or Twitter account.

9 Data Protection

Please refer to our General Data Protection Regulation policies on the website.

10 Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. Mobile phones can be used during lessons to enhance learning, but only in conjunction with this and the Child Protection and Behaviour policies.

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

a. 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 and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access using Google Hangouts);
b. 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;
c. any digital communication between staff and pupils or parents / carers (email, chat, Google Hangout 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;
d. 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 unsuitable communications and be reminded of the need to communicate appropriately when using digital technologies; and
e. personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

11 Social Media - Protecting Professional Identity

Please see the Northumberland PRU Social Media and Guidance Policy.

12 Unsuitable Activities

Northumberland PRU believes that the activities referred to in the following section would be unsuitable 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:

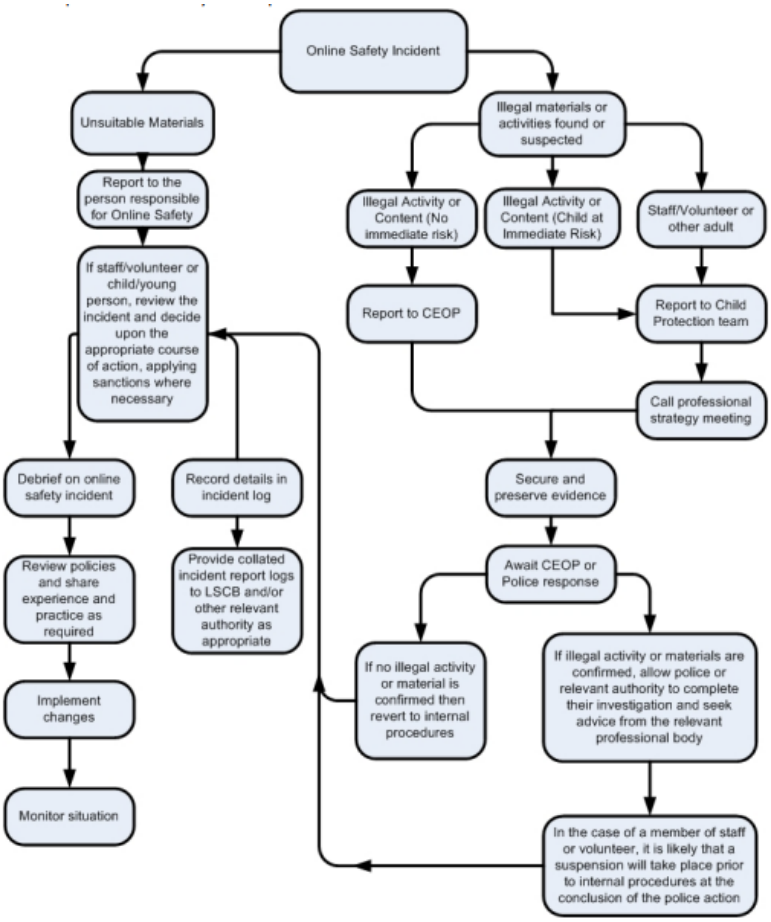
USER ACTIONS		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, social media, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate 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; and				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.					X	
Revealing or publicising confidential or proprietary information (e.g. 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 shopping / commerce.					X	
File sharing.			X			
Use of messaging applications.			X			
Use of video broadcasting e.g. YouTube.			X			

13 Responding to Incidents of Misuse

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 unsuitable activities (see “User Actions” Section 12 above).

13.1 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 Headteacher / police.



13.2 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:

a. Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

b. The designated computer to be isolated and removed from use to preserve evidence and if necessary taken off site by the police should the need arise.

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

d. 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)

e. Once this has been completed and fully investigated, a judgement will be made about the nature of this concern. Appropriate action will be required and could include the following:

    i. internal response or discipline procedures;
    ii. involvement by Local Authority or national / local organisation (as relevant); and
    iii. police involvement and / or action

f. 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:

    i. incidents of ‘grooming’ behaviour;
    ii. the sending of obscene materials to a child;
    iii. adult material which potentially breaches the Obscene Publications Act;
    iv. criminally racist material;
    v. other criminal conduct, activity or materials; and
    vi. 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. Written evidence should be retained by the group for reference purposes by recording it on the sensitive issues confidential log.

13.3 School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve unsuitable 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 the Behaviour or Child Protection Policies.

Appendix A

14. Student Acceptable Use Policy

Every time a pupil logs on to a network computer, they agree (by clicking the agree button) to the ‘Acceptable Use Policy’ which provides guidelines to keep them safe online, without restricting their education.

Although it is difficult to monitor pupils own devices, we have provided a section which encourages them to use their phones, tablets and laptops in a responsible and safe manner.