Newland St. John's C.E. Academy
E-Safety and Acceptable Use Policy

'Living, Learning and Growing in the Love of God.'

Introduction

The school recognises that the Internet and other digital technologies have an important role in the learning and teaching process and aims to provide opportunities for enhancing children's learning through access to these technologies. It is important to balance the benefits with an awareness of the potential risks. Our *E-Safety and Acceptable Use Policy* reflects the school's commitment to the safeguarding and well-being of our pupils.

Responsibilities of the School Community

We believe that E-Safety is the responsibility of the whole school community, and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Senior Leadership Team

- Develop and promote an E-Safety culture within the school community.
- Support the E-Safety coordinator/ Inclusion manager in their work.
- Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to E-Safety effectively.
- Receive and regularly review E-Safety incidents logged on CPOMS and be aware of the procedure to be followed should an E-Safety incident occur in school.
- Take ultimate responsibility for the E-Safety of the school community.

Responsibilities of the E-Safety Coordinator

- Promote an awareness and commitment to E-Safety throughout the school.
- Be the first point of contact in school on all E-Safety matters.

- Create and maintain E-Safety policies and procedures, with the support of other members of staff.
- Develop an understanding of current E-Safety issues, guidance and appropriate legislation.
- Ensure that E-Safety education is embedded across the curriculum.
- Ensure that E-Safety is promoted to parents and carers.
- Liaise with appropriate staff in school, the local authority, the local safeguarding children's board and other relevant agencies as appropriate.
- Monitor and report on E-Safety issues to the Senior Leadership Team as appropriate.
- Ensure any E-Safety incidents are recorded on CPOMS.

Responsibilities of Teachers and Support Staff

- Read, understand and help promote the school's E-Safety policies and guidance.
- Read, understand and adhere to the school staff *Acceptable Use Policy* (AUP).
- Develop and maintain an awareness of current E-Safety issues and guidance.
- Model safe and responsible behaviours in their own use of technology.
- Embed E-Safety messages in learning activities where appropriate.
- Supervise pupils carefully when engaged in learning activities involving technology.
- Be aware of what to do if an E-Safety incident occurs.
- Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Technical Support Staff

- Read, understand and adhere to the school staff AUP.
- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Support the security of the school computing systems.
- Report any E-Safety-related issues that come to their attention to the E-Safety coordinator.
- Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Pupils

- Read, understand and adhere to the school pupil AUP.
- Help and support the school in creating E-Safety policies and practices; and adhere to any policies and practices the school creates.

Responsibilities of Parents and Carers

- Help and support the school in promoting E-Safety.
- Read, understand and promote the school pupil AUP with their children.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies that their children use in school and at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies

- Discuss E-Safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in their own use of technology.
- Consult with the school if they have any concerns about their children's use of technology.

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's E-Safety policies and guidance.
- Support the work of E-Safety in school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in E-Safety activities.
- Ensure appropriate funding and resources are available for the school to implement the E-Safety strategy.

Responsibilities of Visiting Users

- Read, understand and adhere to the school staff AUP and report any E-Safety issues.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the Internet brings.

- We will provide specific E-Safety related lessons in each year group as part of the Computing and PSHCE curriculum.
- We will celebrate and promote E-Safety through whole school Worship.
- We will discuss, remind or raise relevant E-Safety messages with pupils routinely wherever suitable opportunities arise; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
- We will remind pupils about their responsibilities through an AUP which every pupil will sign and will be displayed throughout the school.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:

- Include useful links and advice on E-Safety in newsletters and on our school website
- Ensure a copy of the E-Safety policy is easily accessible.

Managing Computing Systems and Access

The school will be responsible for ensuring that access to the computing systems is as safe and secure as reasonably possible.

- Servers and other key hardware or infrastructure will be located securely.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date.
- The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.
- All users will sign an AUP provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school computing systems, and that such activity will be monitored and checked.
- Pupils will access computers using an individual log-on, which they will keep secure. Internet access will be supervised by a member of staff.
- Members of staff will access the Internet using an individual staff log-on, which they will keep secure. They will ensure they log-out after each session, and not allow pupils to access the Internet through their log-on. They will abide by the school AUP at all times.
- Any administrator or master passwords for school computing systems should be kept secure and available to at least two members of staff.
- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur.
- The school will regularly audit computing use to establish if the *E-Safety Policy* is adequate and that the implementation of the *E-Safety Policy* is appropriate. We will regularly review our Internet access provision, and review new methods to identify, assess and minimize risks.

Filtering Internet access

- The school uses a filtered Internet service. The filtering is provided through PrimaryTec. The class laptops/chrome books and iPads use Kids Rex safe internet search engine.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the E-Safety coordinator. Pupils can use the 'Hector Protector' icon to temporarily block inappropriate content.
- If users discover a website with potentially illegal content, this should be reported immediately to the E-Safety coordinator. The school will report this to appropriate agencies including the filtering provider, LA, Internet Watch Foundation (IWF) or Child Exploitation and Online Protection Centre (CEOP).
- Filtering and other security systems will be reviewed to ensure they meet the needs of all users. Staff can request unblocking of appropriate websites via the PrimaryTec online fault reporter.

- Internet usage is monitored through Smoothwall. Any inappropriate use is reported on a report that is generated daily.

Learning technologies in school

	Pupils	**Staff**
Personal mobile phones brought into school	Allowed with permission	Allowed
Mobile phones used in lessons	Not allowed	Allowed at certain times and to take photos to be added on to social media/website. (e.g. educational visits)
Mobile phones used outside of lessons	Not allowed	Allowed at certain times at the discretion of the Headteacher (staff room)
Taking photographs or videos on personal equipment	Not allowed	allowed to take pictures for social media/website but need to be deleted as soon as the photos are added to social media/website.
Taking photographs or videos on school devices	Allowed	Allowed
Use of hand-held devices such as PDAs, MP3 players or personal gaming consoles	Allowed with supervision	Allowed at certain times
Use of personal email addresses in school	Not allowed	Allowed
Use of school email address for personal correspondence	Not allowed	Allowed
Use of online chat rooms	Not allowed	Not allowed, with the exceptions of 'hangout' on google mail.
Use of instant messaging services	Not allowed	Allowed at certain times
Use of blogs, wikis, podcasts or social networking sites	Allowed at certain times with supervision	Allowed at certain times
Use of video conferencing or other online video meetings	Allowed at certain times with supervision	Allowed at certain times

Using e-mail

- Staff and pupils should use approved e-mail accounts allocated to them by the school and be aware that their use of the school e-mail system may be monitored and checked.
- Key Stage 2 classes will be allocated an individual e-mail account for use by pupils within that class, under supervision of the class teacher.
- Pupils will be reminded when using e-mail about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening e-mail from an unknown sender, or viewing/opening attachments.
- Pupils are not permitted to access personal e-mail accounts during school.
- Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.

Using images, video and sound

- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Digital images, video and sound will only be created using equipment provided by the school or a safe/reliable source.
- Staff and pupils will follow the school policy on creating, using and storing digital resources.
- In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff/parents of pupils involved. Class photo/media permission is obtained from parents when children start school and will be updated and circulated to staff regularly.

Using video conferencing and other online video meetings

We may use video conferencing (such as Skyping) to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. In such instances we will ensure that staff and pupils take part in these opportunities in a safe and responsible manner.

- All video conferencing activity will be supervised by a suitable member of staff.
- Pupils will not operate video conferencing equipment, or answer calls, without permission from the supervising member of staff.
- Video conferencing equipment will be switched off and secured when not in use/online meeting rooms will be closed and logged off when not in use.
- Pupils will be given appropriate user rights when taking part in an online meeting room. They will not have host rights or the ability to create meeting rooms.
- Video conferencing should not take place off school premises without the permission of the head teacher.
- Parental permission will be sought before taking part in video conferences.

- Permission will be sought from all participants before a video conference is recorded. Video conferences should only be recorded where there is a valid educational purpose for reviewing the recording. Such recordings will not be made available outside of the school.

Using new technologies

- As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an E-Safety point of view.
- We will regularly amend the E-Safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an E-Safety risk.

Protecting personal data

We will ensure personal data is 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.

The school will 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)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- 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. Staff will ensure they properly log-off from a computer terminal after accessing personal data.
- Staff will not remove personal or sensitive data from the school premises without permission of the Headteacher, and without ensuring such data is kept secure.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies 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 students / 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's use of social media for professional purposes will be checked regularly by the senior risk officer and E-Safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

The school website and other online content published by the school

- The school website will not include the personal details, including individual e-mail addresses or full names, of staff or pupils.
- A generic contact e-mail address will be used for all enquiries received through the school website.
- All content included on the school website will be approved by the Senior Leadership Team.

- Staff and pupils should not post school-related content on any external website without seeking permission first.

Dealing with E-Safety incidents

In most situations, where a member of staff is made aware of a possible E-Safety incident, they should log the incident on CPOMS.

Lyn Frankton - Inclusion Manager including E- Safety Coordinator in conjunction with Nick Rouse - IT Coordinator

Date of next review – November 2022

Appendices

Appendix 1 - Acceptable Use Policy for staff and other adults in school

These statements are designed to ensure staff and other adults in school are aware of their professional responsibilities when using the Computing systems provided. All staff should follow the guidelines at all times. You are responsible for your behaviour and actions when accessing the Internet at school, whether on your own or school equipment, and when using school Computing equipment at other locations such as your home.

- Any use of school computing systems will be for professional purposes as agreed by the school senior management team
- Usernames, passwords and other logon details should be kept secure and not revealed to anyone else. Care should be taken to ensure you logout when not actively using the computing systems. You should not allow an unauthorised person to access the school computing systems, e.g. by logging in for them.
- Any online activity should not harass, harm, offend or insult other users.
- You will not search for, download, upload or forward any content that is illegal, or that could be considered offensive by another user. If you accidentally encounter such material you should follow your school's procedure and report this immediately.

- You should not download or install any hardware, software or apps without permission. If you have responsibility for installing software you should be confident it is adequately licensed and appropriate for educational use.
- Any electronic communications should be related to schoolwork only. It is not acceptable to contact pupils or parents using personal equipment or personal contact details including your own mobile phone or through your personal social network profiles.
- Any online activity, including messages sent and posts made on websites, and including activities outside of school, should not bring your professional role or the name of the school into disrepute.
- Any still or video images of pupils and staff should be for professional purposes only.
- You will not give out your personal details, or the personal details of other users, to pupils or parents or on the Internet. In particular you should ensure your home address, personal telephone numbers and email accounts are not shared with children, young people or parents.
- You should ensure that any personal or sensitive information you use or access (e.g. SIMS data, assessment data) is kept secure and used appropriately.
- Personal or sensitive information should only be taken off-site if agreed with the Headteacher, and steps should be taken to ensure such data is secure.
- You should respect intellectual property and ownership of online resources you use in your professional context, and acknowledge such sources if used.
- You should support and promote the school *E-Safety Policy*, and promote and model safe and responsible behaviour in pupils when using technology to support learning and teaching
- You understand that your files, communications and Internet activity may be monitored and checked at all times to protect your own and others' safety, and action may be taken if deemed necessary to safeguard yourself or others. If you do not follow all statements in this AUP and in other school policies you may be subject to disciplinary action in line with the school's established disciplinary procedures.

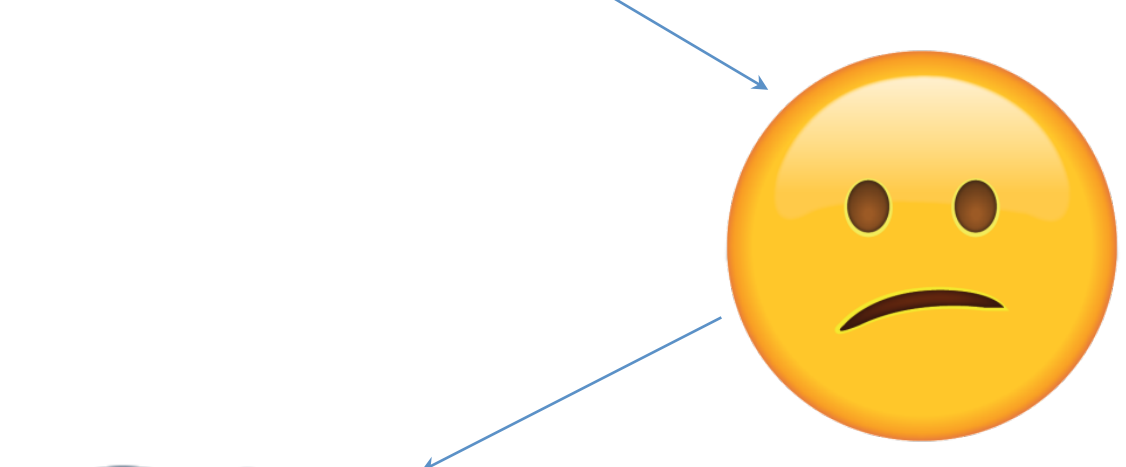
I have read and understand the above and agree to use the school computing systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name	
Signed	
Date	

Appendix 2 - Acceptable Use Policy for children and young people in school

NEWLAND ST JOHN'S C OF E ACADEMY

Our Acceptable Use Charter



NEWLAND ST JOHN'S C OF E ACADEMY

Our Acceptable Use Charter – KS1

- I understand that there are different ways of communicating.
- I only open and send emails with a grown up.
- I only open emails from somebody I know.
- I know that websites sometimes have pop-ups that take me away from where I want to be.
- I know that not all websites tell the truth.
- I know that not all people on the internet tell the truth.
- I can keep my personal information private and not share it online.
- I only use the search engines the teacher has told me to.

- I use Hector and tell a grown up straight away if I see something I am unsure about.
- I can use a password to log in to my account.

NEWLAND ST JOHN'S C OF E ACADEMY

Our Acceptable Use Charter – LKS2

- I recognise when a website or person on the internet isn't being truthful.
- I understand I need to be cautious when searching on the internet, and I know how to report something I am unsure about and how to use Hector.
- I understand that search engines will give different results at home than when at school.
- I understand that I need to keep personal information and passwords private.
- I understand that I may have to use an alias to keep my identity safe.
- I can identify when emails should not be opened and when an attachment may not be safe.
- I can use a password to log in to my accounts.

- I understand that anything I share online can be seen and used by others.
- I know how to respond if somebody on the internet is making feel unsafe or unhappy.

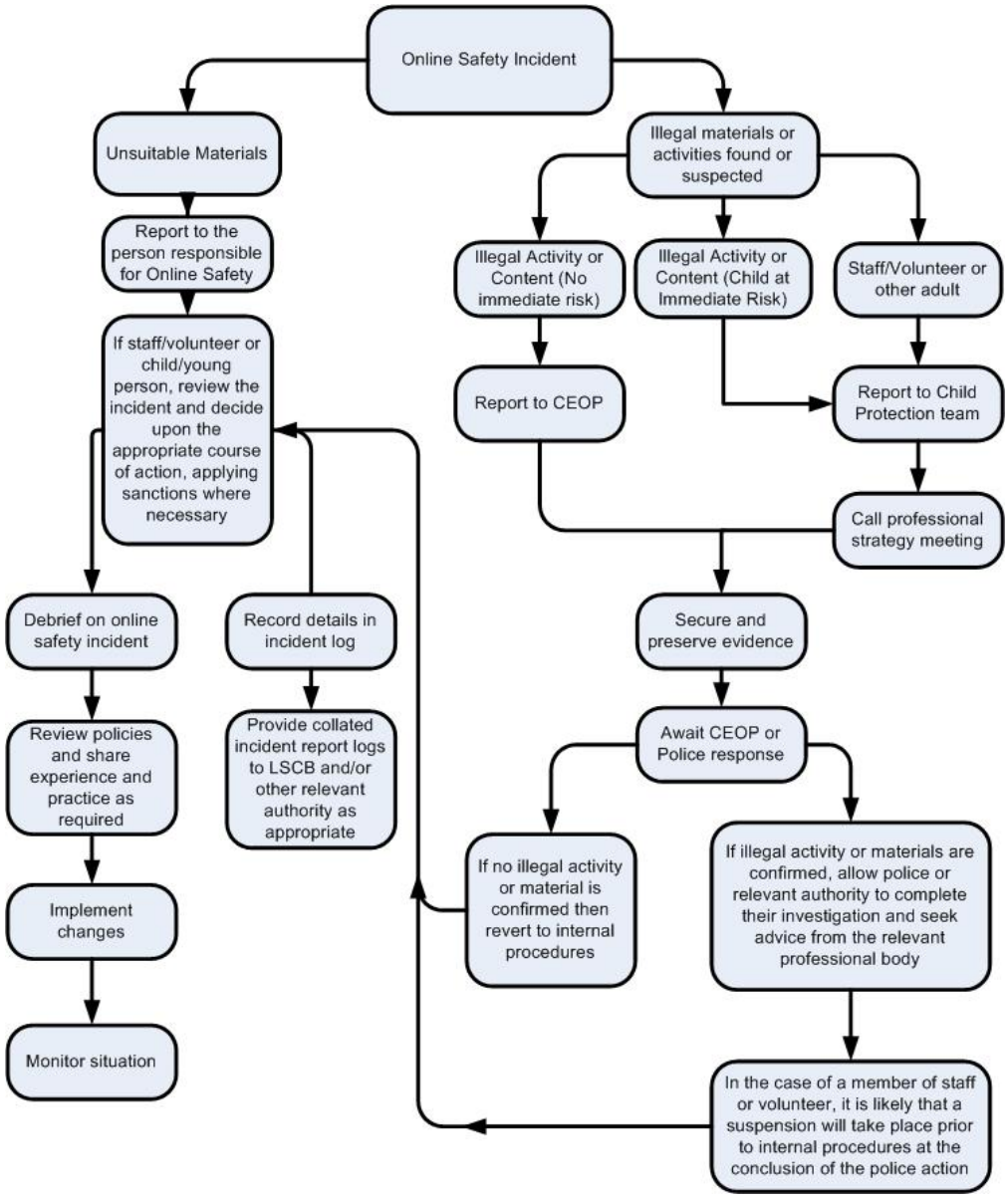
NEWLAND ST JOHN'S C OF E ACADEMY

Our Acceptable Use Charter – UKS2

- I understand the risks of sharing information online.
- I understand how to minimise the risks of online communication.
- I understand that some online environments have security settings which can be altered to protect me.
- I understand that some people on the internet may deliberately try to trick me for my personal information.
- I know that it is unsafe to meet unknown people I've met online.
- I know how to report anything I am unsure about, including using Hector.
- I understand that I should not share people's pictures or tag them on the internet without their permission.
- I understand that once I have shared something online it is difficult to remove.

- I know how to respond if somebody on the internet is making feel unsafe or unhappy.
- I can choose safe ways to communicate on the internet.
- I know how to create a strong password, and how to manage this.

Appendix 3 - Responding to E-Safety incidents – flow chart



Appendix 4 - Staff Procedures Following Misuse by Staff

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by an adult:

A. An inappropriate website is accessed inadvertently:
Log incident on CPOMS.
Contact the helpdesk of the filtering service for school so that it can be added to the banned or restricted list. Change Local Control filters to restrict locally.
Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:
Ensure that no one else can access the material by shutting down.
Log the incident. Report to the Headteacher and E-Safety Leader immediately.
Headteacher to refer back to the *Acceptable Use Policy* and follow agreed actions for discipline. Inform the filtering services as with A.

C. An adult receives inappropriate material:
Do not forward this material to anyone else – doing so could be an illegal activity. Alert the Headteacher immediately. Ensure the device is removed and log the nature of the material. Contact relevant authorities for further advice e.g. police.

D. An adult has used Computing equipment inappropriately:
Follow the procedures for B.

E. An adult has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately, if necessary. Report to the Headteacher and Designated Person for Child Protection immediately, who should then follow the Allegations Procedure and Child Protection Policy from Section 12, LSCBN. Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent. Once Procedures and Policy have been followed and the incident is considered innocent, refer to the *Acceptable Use Policy* for Staff and Headteacher to implement appropriate sanctions. If illegal or inappropriate misuse is known, contact the Headteacher or Chair of Governors (if allegation is made against the Headteacher) and Designated Person for Child Protection immediately and follow the Allegations procedure and Child Protection Policy. Contact CEOP/police as necessary.

F. Threatening or malicious comments are posted to the school website (or printed out) about an adult in school:

Preserve any evidence. Inform the Headteacher immediately and follow *Child Protection Policy* as necessary. Inform the LA and e-Safety coordinator so that new risks can be identified. Contact the police or CEOP as necessary.
Remove comments from website.

G. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted e.g. on Social Media:
Report to the Headteacher.

Appendix 5 - Staff Procedures Following Misuse by Children and Young People

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by a child or young person:

A. An inappropriate website is accessed inadvertently:
Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult. Report website to the E-Safety coordinator if this is deemed necessary. Contact the helpdesk filtering service for school so that it can be added to the banned list or use Local Control to alter within your setting. Check the filter level is at the appropriate level for use in school.

B. An inappropriate website is accessed deliberately:
Refer the child to the *Acceptable Use Policy* that were agreed. Reinforce the knowledge that it is illegal to access certain images and police can be informed. Decide on appropriate sanction. Notify the parent/carer. Inform helpdesk as above.

C. An adult or child has communicated with a child or used Computing equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately. Report to the Headteacher and Designated Person for Child Protection immediately. Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent. Contact CEOP/police as necessary.

D. Threatening or malicious comments are posted to the school website about a child in school:
Preserve any evidence. Inform the Headteacher immediately. Inform the LA and E-Safety coordinator so that new risks can be identified. Contact the police or CEOP as necessary. Remove comments from website.

E. Threatening or malicious comments are posted on external websites about any member of the school community:
Preserve any evidence. Inform the Headteacher immediately.

N.B. There are three incidences when you must report directly to the police.

- **Indecent images of children found.**
- **Incidents of 'grooming' behaviour.**
- **The sending of obscene materials to a child.**

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found.
They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately. If in doubt, do not power down the machine.
Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image. www.iwf.org.uk provide further support and advice in dealing with offensive images online.

Appendix 6 - Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students / Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people can not be identified by the use of their names.

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 / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Parents / carers are requested to sign the permission form (available in the office) to allow the school to take and use images of their children and for the parents / carers to agree.