Duston Eldean Primary School

'TOGETHER WE GROW'

At Duston Eldean we encourage a creative, caring and respectful environment where the whole school community is happy, enthused and motivated.

In developing a love for learning we sow the seeds of success.

Acceptable Use Policy

Signed …… Signed ……

(Chair of Governors) (Head teacher)

Date …… Date ……

Date of Adoption:

Frequency of Review: Annual

Review Date due:

Acceptable Use Policy for School Employees 2020/21

1. Policy Statement

In order to create a safe teaching and learning environment, effective policies and procedures which are clearly understood and followed by the whole school community are essential. This Acceptable Use Policy sets out the roles, responsibilities and procedures for the safe and appropriate use of all technologies to safeguard adults, children and young people within a school or educational setting.

The purpose of the Acceptable Use Policy is to clearly identify for the whole school community:

i) the steps taken in school to ensure the safety of pupils when using the internet, e-mail and related technologies.

ii) the school's expectations for the behaviour of the whole school community whilst using the internet, e-mail, social media and related technologies within and beyond school.

iii) the school's expectations for the behaviour of staff when accessing and using data.

2. Scope of policy

The policy applies to all school-based employees, including individuals working in a voluntary capacity. All schools are expected to ensure that non-employees on site are made aware of the expectation that technologies and the internet are used safely and appropriately. The Acceptable Use Policy should be used in conjunction with the school's disciplinary procedures and code of conduct applicable to employees and pupils.

Where this policy is applied to the Head Teacher, the Chair of Governors will be responsible for its implementation.

3. Legal background

All adults who come into contact with children and young people in their work have a duty of care to safeguard and promote their welfare. The legal obligations and safeguarding duties of all school employees in relation to use of technologies feature within legislative documents such as:

Working Together to Safeguard Children 2018
Safeguarding Vulnerable Groups Act 2009
Keeping Children Safe in Education 2018
Counter Terrorism and Securities Act 2015

All safeguarding responsibilities of schools and individuals referred to within this Acceptable Use Policy includes, but is not restricted to the legislation listed above.

4. Responsibilities

Head Teacher and Governors
The Head Teacher and Governors have overall responsibility for e-Safety as part of the wider remit of safeguarding and child protection. To meet these responsibilities, the Head Teacher and Governors should:

- designate an e-safety lead to implement agreed policies, procedures, staff training (including new starters), curriculum requirements and take the lead responsibility for ensuring e-safety is

addressed appropriately. All employees, students and volunteers should be aware of who holds this post within school.

- provide a safe, secure and appropriately filtered internet connection for staff, children and young people within the school.

- provide resources and time for the e-safety lead and employees to be trained and update protocols where appropriate.

- promote e-safety across the curriculum and have an awareness of how this is being developed, linked with the school development plan.

- ensure that any equipment which holds sensitive or confidential information and leaves school premises (e.g. staff laptops and memory sticks) are either password protected or encrypted.

- share any e-safety progress and curriculum updates at governing body meetings and ensure that all present understand the link to child protection.

- ensure that e-safety is embedded within all child protection training, guidance and practices.

- elect a designated Governor to challenge the school about e-safety issues.

E-Safety Lead
The nominated e-safety lead should:

- recognise the importance of e-safety and understand the school's duty of care for the safety of their pupils and employees.

- establish and maintain a safe ICT learning environment within the school.

- with the support of the ICT technician, ensure that filtering is set to the correct level for employees, young volunteers, children and young people accessing school equipment.

- Through maintenance of an incident log, report issues of concern and update the Head Teacher and governing body on a regular basis.

- liaise with Anti-Bullying lead and DSL so that procedures are updated and communicated, and take into account any emerging e-safety issues and technological changes.

- co-ordinate and deliver employee training according to new and emerging technologies so that the correct e-safety information is being delivered.

- with the support of the ICT technician, implement a system of monitoring employee and pupil use of school issued technologies and the internet where appropriate .

Code of Conduct-
All school based employees, including volunteers, must:

- take responsibility for their own use of technologies and the internet, making sure that they are used legally, safely and responsibly.

- ensure that children and young people in their care are protected and supported in their use of technologies so that they can be used in a safe and responsible manner (see appendix 3).

- report any e-safety incident, concern or misuse of technology to the e-safety lead, Head Teacher or DSL, including the unacceptable behaviour of other members of the school community.

- only use school ICT systems and resources for all school related business and communications involving sensitive pupil data or information.

- due to equipment shortages, personal technology such as mobile phones and i-pads may be used to take photographs/videos/audio recording (digital artefacts) of children engaged in school related activities only. The purpose of the image/video/recording should be to support children's learning or for sharing through official communication channels (i.e. school facebook account, twitter, parent mail, Itslearning, Tapestry). These images must only be taken on a personal device if authorised by a member of ELT. Once shared for the intended purpose, the digital artefact must be correctly and permanently deleted from the device.

- ensure that all electronic communication with pupils, parents, carers, employees and others is compatible with their professional role and in line with school protocols. Personal details, such as mobile number, social network details and personal e-mail should not be shared or used to communicate with pupils and their families.

- not post online any text, image, sound or video which could upset or offend any member of the whole school community or be incompatible with their professional role. Individuals working with children and young people must understand that behaviour in their personal lives may impact upon their work with those children and young people if shared online or via social networking sites.

- not invite, accept or engage in communications with children from the school community (past or present) on any personal social networking sites.

- protect their passwords/personal logins and log-off the network wherever possible when leaving work stations unattended.

- understand that network activity and online communications on school equipment (both within and outside of the school environment) may be monitored, including any personal use of the school network.

- understand that employees, who ignore security advice or use email or the internet for inappropriate reasons, risk dismissal and possible police involvement if appropriate.

- [*applicable to members of staff only*] When investigating claims of cyberbullying/online abuse, a child's mobile device (if onsite) can be looked at to ascertain correct information to help with the investigation. In this situation, the child and another member of staff should be present when looking at the device. Where possible, ask the child to show you only the information that you are looking for. A parent/guardian should be notified that this incident has taken place. If the device is not onsite, notify parents/guardians to guide them to the information that is needed, or request they bring in the device to help in dealing with the situation.

Acceptable use of Technology Agreement should be signed on appointment by all staff members (See Appendix 1) When joining the school, parents/carers will be given a copy of an Acceptable Use Agreement seeking permission for their children to access the internet. (See Appendix 2)
Children are taught rules to ensure their safety when online and sign an agreement. (See Appendix 3)

5. Inappropriate Use

Examples of inappropriate use include:

- accepting or requesting pupils as 'friends' on social networking sites, or exchanging personal email addresses or mobile phone numbers with students.

- behaving in a manner online which would lead any reasonable person to question an individual's suitability to work with children or act as a role model.

In the event of staff misuse
If an employee is believed to have misused the internet or school network in an illegal, inappropriate or abusive manner, a report must be made to the Head teacher/Safeguarding lead immediately. The appropriate procedures for allegations must be followed and the following teams/authorities contacted:

- EPM (Human Resources)
- Designated Officer (Formerly known as LADO- Local Authority Designated Officer)
- Police/CEOP (if appropriate)

Please refer to the Online Safety Incident Flowchart (Appendix 4) and procedures following misuse by staff. (Appendix 5)

In the event of minor or accidental misuse, internal investigations should be initiated and staff disciplinary procedures followed if appropriate.

Potential and Actual Breaches of the Code of Conduct
In instances where there has been a breach of the above Code of Conduct, the following will apply:

- Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy, this may result in action being taken under the Disciplinary Procedure. A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school's ethos and principles.

- The Governing Body will take appropriate action in order to protect the school's reputation and that of its staff, parents, governors, children and anyone else directly linked to the school.

In the event of inappropriate use by a child or young person
In the event of access to inappropriate materials, students are expected to notify an adult immediately.

Students should recognise the CEOP Report Abuse button (www.thinkuknow.co.uk) as a place where they can make confidential reports about online abuse, sexual requests or other misuse which they feel cannot be shared with teachers.

Please refer to Procedures following Misuse by Children/Young People (Appendix 6)

6. Policy Review

The Acceptable Use Policy will be updated to reflect any technological developments and changes to the school's ICT Infrastructure. Acceptable Use Rules for students should be consulted upon annually by the school community to ensure that all young people can understand and adhere to expectations for online behaviour.

7. Useful Links

https://www.nasuwt.org.uk/advice/health-safety/social-media-the-abuse-of-technology/protecting-your-privacy-online.html NASUWT Social Networking- Guidelines for Members)

https://neu.org.uk/advice/online-safety-protecting-school-staff-and-pupils
(NUT E-Safety: Protecting School Staff- Guidance for Members)

https://www.ceop.police.uk/safety-centre/
(reporting system for children, parents and professional)

www.thinkuknow.co.uk
(information and resources for children, teenagers, parents/carers and professionals)

https://www.childnet.com/resources (resources from professionals and teachers)

https://www.net-aware.org.uk/ (social media guide for professional and teachers)

https://www.commonsensemedia.org/
(Advice for parents and professionals on children's entertainment including apps, games and movies)

T:\2. Curriculum Resources\Esafety Curriculum
(Online safety curriculum resources on staff share)

Appendix 1 - Staff Acceptable Use of Technologies Agreement

To ensure that all staff are confident in their use of technologies and the internet, the Acceptable Use Rules have been developed in collaboration with education professionals and unions. The core values of the Acceptable Use Policy are safeguarding and responsible behaviours allowing young people, and the adults who surround them, to safely enjoy all of the benefits that technology can offer. To assist with this, the full Acceptable Use Policy is accessible to all staff members and should be referred to for further information.

The Online-Safety Lead is: Stacey Ramm (ICT/Computing Lead))

The Designated Safeguarding Leads for Child Protection are:

Cathy Moore (Head Teacher)
Andy Stevenson (Deputy Head Teacher)
Emma Bateman (Family Liaison Officer)
Jane Other and Katie Jones
(Safeguarding Governors)

- I know that I should only use the school equipment in an appropriate manner and for professional use, unless otherwise agreed by the Head Teacher.
- I understand that I must not have personal communications with current, or former pupils, outside of my professional role. This includes establishing social networking 'friendships' on sites such as Facebook, or sharing personal phone numbers or email addresses. Any school related communication should be conducted through professional email accounts or telephone numbers only.
- I understand that I should not behave in a manner, either within or outside of the work environment, which would lead any reasonable person to question my suitability to work with children or act as a role model. This would include inappropriate comments, photographs or videos on social networking sites which reflect badly on myself, my colleagues or the school.
- I know that permission must be received from parents/carers before images of children are used online (e.g. school website). I understand that images must be appropriate and should not reveal any personal information, including first names given on social media sites.
- In the event that a personal device is used to take photographs or videos, the digital artefact created must be authorised by a member of ELT and permanently disposed of as soon as possible.
- I understand that any incidents of concern for children's safety must be reported to the Head Teacher, Designated Safeguarding Leads for Child Protection or E-safety Lead in accordance with procedures listed in the Acceptable Use Policy
- I know where to access a copy of the Online Safety Incident Flowchart should an incident of misuse arise.
- I understand that the school email system and school issued devices could be monitored as part of our commitment to safeguard young users.
- I know that each user should be accessing the internet with their unique username and password for filtering and safeguarding purposes. For this reason, I will keep my password private and for my own use only.
- I will raise any concerns regarding school ICT use with my line manager to avoid possible misunderstandings.

- I have access to a copy of the full Acceptable Use Policy should I need to refer to the document about any online-safety issues or procedures.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will notify parents/ carers when I have had to look on a child's device when investigating an online safety incident.

I have read, understood and agree to the above Acceptable Use rules. I understand that these rules are in place to ensure that staff are aware of their professional responsibilities to safeguard children when accessing online technologies.

Signed: …….. Dated: ……

Appendix 2 – Parent/Carer Acceptable Use of Technologies Agreement

Accessing the internet
As part of an enriched curriculum, your child will be accessing the internet, school email and virtual learning environment via a filtered service provided by Talk Straight Ltd.. In order to support the school in educating students about safe use of the internet, we are asking parents and children to read and sign acceptance of the attached acceptable use rules. Completed forms should be returned to the school as soon as possible.

The rules provide an opportunity for further discussions with your child about safe and appropriate use of the internet and other online tools (e.g. mobile phones), both within and beyond school (e.g. at a friend's house or at home). Sanctions in place for misuse of technologies and subsequent breach of the rules are detailed in the full Acceptable Use of Technologies Policy which parents/carers are welcome to view.

Further Information and Guidance

- https://www.ceop.police.uk/safety-centre/ (reporting system)
- www.thinkuknow.co.uk
- https://www.childnet.com/resources
- https://www.net-aware.org.uk/ (social media guide for professional and teachers)

Social Media
Digital technologies have become an important part of our lives. These technologies provide powerful tools which open up new opportunities for everyone. As such, we have established a Twitter and Facebook account for the school. Through the use of social media, we hope to help parents facilitate discussions with their children about the school day, celebrate the teaching and learning within the school and model best practice in how to navigate social media safely and effectively.

Our social media is not intended to replace face to face discussions with members of staff and any worries or concerns should be communicated in person, by telephone or by emailing bursar@dustoneldean.northants-ecl.gov.uk

Please note, in order to safely manage these accounts and protect anonymity:

- You will be unable to post anything to the wall (only comment on what the school has posted)
- You will be unable to private message the school through Facebook or Twitter
- You will be unable to 'tag' us into any of your personal posts.
- We will use class names but will not name any individual children.

We intend to post pictures of children in school at work and also outside on school trips. Please indicate on the form below whether or not you give consent for your child to have photographs on our school website, Facebook and Twitter accounts.

If you would like to discuss any reservations before giving permission, please speak to Miss Stacey Ramm, our E-safety Lead (Year 4 Jaguars).

Please note, we expect only adults to follow/like any posts submitted on social media. The table below lists current social media platforms and their minimum age restrictions.

Social Media Platform	Minimum Age	Social Media Platform	Minimum Age
Facebook	13+	Twitch	13+
Instagram	13+	Twitter	13+
Kik	13+	Viber	13+
Omegle	13+	Whatsapp	16+
Roblox	7+	Youtube	13+
Snapchat	13+		
Tiktok	13+		

Devices within school

Children from Year 5 onwards are permitted to bring in a mobile device to school. Children should only bring in these devices if they are walking to and from school. If children are not walking to school, we would expect these devices to stay at home.

When devices are bought into school, they will be switched off once they are on school grounds. Devices are handed into class teachers, who lock them away in a secure place. These are then retrieved at the end of the day, where they are not to be switched on until off school grounds.

In the event of a reported online safety issue and the device is in school, the school may check your child's device with your child and another member of staff present. Parents/guardians will be notified that this has occurred.

Wearable Technology

As a school, we encourage children to be aware of their health and their physical activity. We allow children to wear devices that help count their steps throughout the day. Digital watches are also permitted, but all associated alarms should be turned off during the school day.

We do not allow devices which are internet enabled or communicative in anyway.

We look forward to sharing our school day with you.

Many thanks

Miss Stacey Ramm and Mrs Cathy Moore

Permission slip re: Accessing the internet and Social Media

Childs Name:

Class:

Accessing online - Parent/Carer Agreement:

- I have read and discussed the rules with my child and confirm that he/she has understood what the rules mean.

- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the internet, email and other online tools.

- I understand that filtering can never be completely fool proof and occasionally inappropriate materials may be accessed. I accept that the school will endeavour to deal with any incident that may arise swiftly and according to policy.

- I understand that my child's safe use of the internet and online technologies outside of school is my responsibility.

Social Media

- ☐ I do give permission for my child's photograph to be used on the school website and social media accounts, throughout their time at Duston Eldean Primary School.

- ☐ I do not give permission for my child's photograph to be used on the school website and social media accounts, throughout their time at Duston Eldean Primary School.

Devices in school (Yr5 + Yr6 parents/guardians only)

- I understand that mobile devices should only be sent into school if my child is walking to and from school

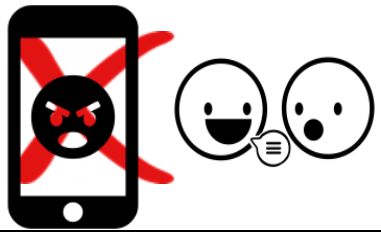
- I understand that any device bought into school is switched off and locked away during the school day.

- I understand that any wearable technology that is internet enable or can be used as a communicative device should not be bought into school.

Parent/Carer Signature: _____ Date: _____

Appendix 3 - Child Acceptable Use of Technologies Agreement

I know to stay safe, I have to think **SMART.**

S- Safe	
✓ I will not give out my name, address or personal information to anyone I meet online. ✓ I will only share my passwords with my trusted adults. ✓ I understand that when I am in school, what I see online can be seen by adults to help keep me safe.	
M- Meeting	
✓ I will tell my trusted adults if someone asks to meet me online. I understand this can be dangerous so adults will need to sort this for me.	
A- Accepting	
✓ Accepting files, emails, pictures or text messages from places you do not know can lead to problems. They could have viruses on them. ✓ If I am unsure I will tell a trusted adult before I do anything.	
R-Reliable	
✓ Information I see on the internet might not be true. Sometimes people lie about facts and even about who they are. ✓ I will be careful not to trust everything and speak to a trusted adult if I am unsure.	
T- Tell	
✓ If I feel worried or a bit funny about something I see online, I will tell a trusted adult. ✓ I can also report things that have happened to other people, especially if friends are being bullied online. ✓ I will report any e-safety incident to a trusted adult.	

I understand the rules for using the internet and email safely and responsibly. I know that the adults working with me at school will help me to stay safe and check that I am using the computers to help me with my work.

CLICK CEOP Internet Safety

I can click this button to report things that worry me on the internet

Name: _____**Class:**_____

Child Signature: _____ **Date:** _____

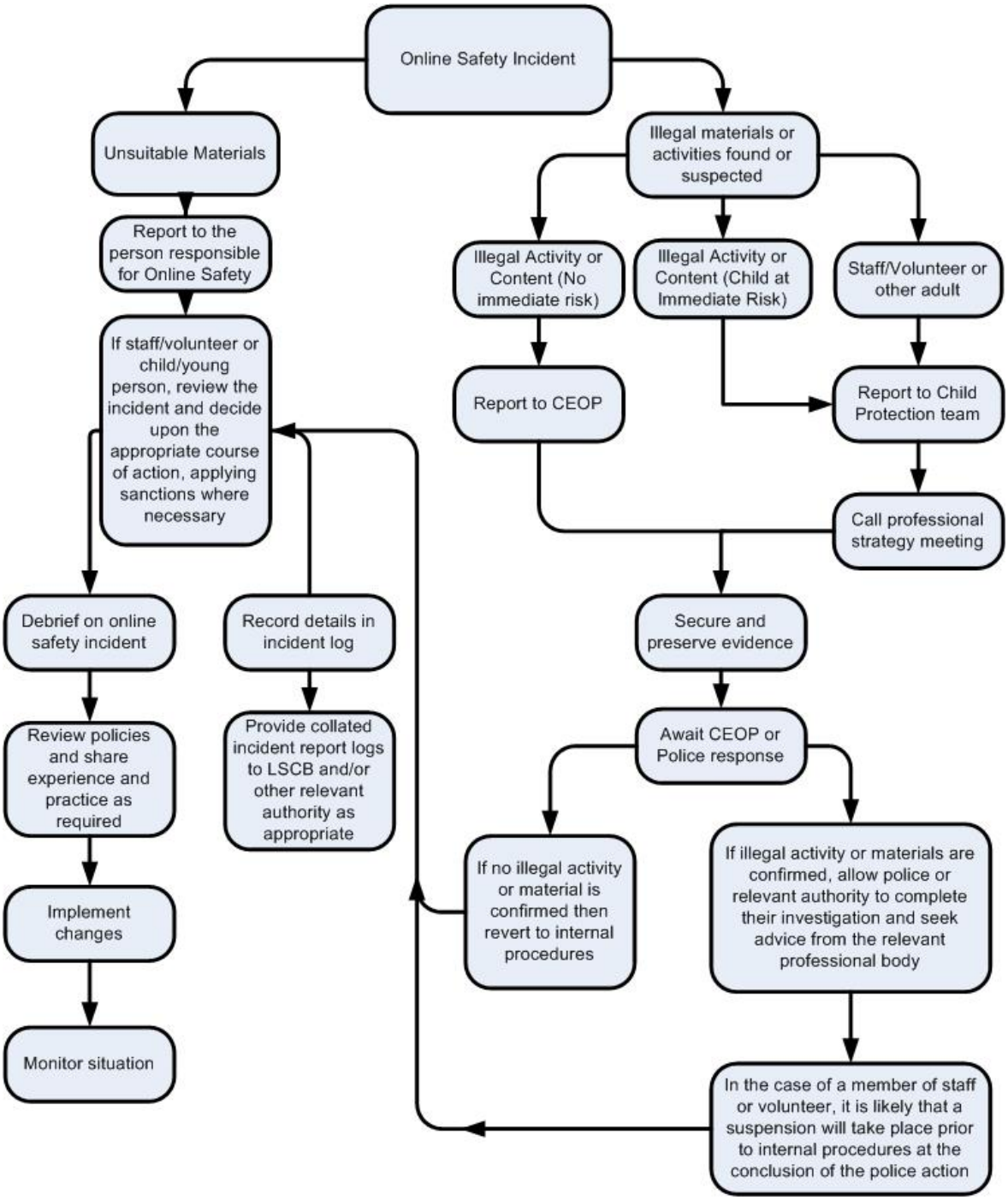
Appendix 4 – Online Safety Incident Flowchart

There are three instances when you must report directly to the police.

- Indecent images of children found (i.e. under 18 yrs of a sexual nature)
- 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. The police 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 turn off the machine. The Internet Watch Foundation www.iwf.org.uk offers further support and advice in dealing with offensive images online.

It is important to remember that any offensive images received should never be forwarded, even if it is to report them as illegal, as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.



Appendix 5- Staff Procedures following Misuse by Staff

The Head Teacher 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:

Report website to the Online Safety Lead if this is deemed necessary. ICT lead will add this site to the banned list immediately.

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 Head Teacher, DSL and E-Safety Leader immediately.
- Head Teacher to refer back to the Acceptable Use Rules and follow disciplinary procedures.

C. An adult receives inappropriate material.

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the Head Teacher 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 ICT 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 Head Teacher and Designated Safeguarding Lead for Child Protection immediately, who should then follow the Allegations Procedure and Child Protection Policy from Section 12, Northamptonshire Safeguarding Board.
- 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 Rules for Staff and Headteacher to implement appropriate sanctions.
- If illegal or inappropriate misuse is known, contact the Head Teacher or Chair of Governors (if allegation is made against the Head Teacher) and Designated Safeguarding Lead 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 learning platform (or printed out) about an adult in school:

- Preserve any evidence.
- Inform the Head Teacher immediately and follow Disciplinary Procedures as necessary.
- Inform the Local Authority's Designated Officer and Online Safety Lead so that new risks can be identified.
- Contact the police or CEOP as necessary.

G. Where staff or adults have posted on inappropriate websites, or have inappropriate information about them posted, this should be reported to the Head Teacher.

Appendix 6- Staff Procedures following Misuse by Children/Young People

The Head Teacher 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 lead if this is deemed necessary.
- E-safety lead will add site to the banned list immediately.

B. An inappropriate website is accessed deliberately:

- Refer the child to the Acceptable Use Rules 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.

C. An adult or child has communicated with a child or used ICT equipment inappropriately:

- Ensure the child is reassured and remove them from the situation immediately.
- Report to the Head Teacher and Designated Safeguarding Lead for Child Protection immediately.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- If illegal or inappropriate misuse the Head Teacher must follow the Allegation Procedure and/or Child Protection Policy from Section 12, Northamptonshire Safeguarding Board.
- 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 Head Teacher immediately.
- Inform the Northamptonshire Safeguarding Board and E-safety lead so that new risks can be identified.
- Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about an adult in the school or setting:

- Preserve any evidence.
- Inform the Head Teacher immediately.