ESTCOTS PRIMARY SCHOOL

E-Safety Policy

e-Safety policy – November 2018
SBM and ICT co-ordinator

Estcots primary School E-Safety Policy

Contents

Appendices:

1. Introduction and overview

Rationale and scope
The purpose of this policy is to:

Our aim in presenting an e-safety policy is to create a safe environment where we can both work and learn. This environment should be safe for both young people and adults alike.

E-safety is not purely a technological issue. The responsibility for e-safety must not be solely delegated to technical staff, or those with a responsibility for computing.

Schools must therefore, firmly embed e-safety within all safeguarding policies and practices. This then makes that responsibility rest with of all those who work with young people whether in a paid or unpaid capacity.

No one policy or technology can create the safe learning and working environment we need. Schools can work towards this by combining the following:

Policies and Guidance include, but are not limited to:

- The school Acceptable Use Policy (AUP)
- The staff Guidance for the Safer Use of the Internet

These policies set the boundaries of acceptable use. Schools need to use these policies, however, in conjunction with other policies including, but not limited to:

- The Behaviour Management Policy
- The Anti-Bullying Charter

The Staff Handbook / Code of Conduct for Staff

- Prevent Duty

Technology Based Solutions include:

- Internet filtering – EXA provides a system, Securus for those schools and academies on the schools network. Establishments not on the schools network will provide their own internet filtering solution.

- ESET Antivirus Software – regularly updated and that is purchased through JSPC.

- ESafe is our “Automatic network monitoring software” which has a triple lock protection approach to monitor daily IT use of all staff and pupils – this is purchased and renewed through JSPC.

Education in terms of acceptable use and responsibility The policy also:

- sets out the key principles expected of all members of the school community at Estcots Primary School with respect to the use of ICT-based technologies;
- safeguard and protect the children and staff of Estcots Primary School;
- assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice;
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use;
- have clear structures to deal with online abuse such as cyber bullying which are cross referenced with other school policies;

• ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken;
• minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

• exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse;
• lifestyle websites, for example pro-anorexia/self-harm/suicide sites;
• hate sites;
• content validation: how to check authenticity and accuracy of online content.

Contact

• grooming;
• cyber bullying in all forms;
• identity theft (including 'frape' (hacking Facebook profiles) and sharing passwords).

Conduct

• privacy issues, including disclosure of personal information;
• digital footprint and online reputation; • health and well-being (amount of time spent online - internet or gaming);
• sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images);
• copyright (little care or consideration for intellectual property and ownership – such as music and film) (Ref. Inspecting E-Safety: new Ofsted Guidance 2013).

Development/monitoring/review

The school has an E-Safety Co-ordinator who will be responsible for document ownership, review and updates.

This Online Safety policy was approved by the Governing Board on:	Mr R Taylor
The implementation of this Online Safety policy will be monitored by the:	E-Safety Co-ordinator and Senior Leadership Team
Monitoring will take place at regular intervals:	Annually
The Governing will receive a report on the implementation of the Online Safety Policy generated by the E Safety Coordinator (which will include anonymous details of online safety incidents) at regular intervals:	Annually
The Online 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 online safety or incidents that have taken place. The next anticipated review date will be:	Autumn Term 2019
Should serious online safety incidents take place, the following external persons / agencies should be informed:	LA Safe Guarding Officer, MASH, LADO, Police

Scope

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

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

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

Roles and Responsibilities

Roles	Key Responsibilities
Headteacher	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered internet Service, which complies with current statutory requirements e.g. Exa • To be responsible for ensuring that staff, especially the e-safety Co-ordinator, receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse). • To receive regular monitoring reports from the E-Safety Coordinator • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures(e.g. network manager)
E-Safety Co-ordinator /Designated Child Protection Leader	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school E-Safety policy • Promotes an awareness and commitment to e-safeguarding throughout the school community • Ensures that e-safety education is embedded across the curriculum • Liaises with school ICT technical staff • the production / review / monitoring of the school Online Safety Policy / documents. • mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression • monitoring network / internet / incident logs • consulting stakeholders – including parents / carers and the students / pupils about the online safety provision • monitoring improvement actions identified through use of the 360 degree safe self-review tool • meet regularly with SLT and the designated Safeguarding Governor to discuss current

	issues, review incident logs and filtering change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • To ensure that an E-Safety Incident Log is kept up-to-date • Facilitates training and advice for all staff • Liaises with the Local Authority and relevant agencies • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: • sharing of personal data • access to illegal/inappropriate materials • inappropriate online contact with adults/strangers • potential or actual incidents of grooming • cyber bullying and use of social media
Governors/ Safeguarding Governor	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety policy and review the effectiveness of the policy. This will be carried out by the governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor, including the e-safety aspect • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include: regular review with the E-Safety Co-ordinator/Officer (including E-Safety incident logs, filtering/change control logs)
Computing & PSHE Curriculum Leader	• To oversee the delivery of the e-safety element of the computing curriculum • To liaise with the E-Safety Co-ordinator regularly
Network Manager/ Technician	• To report any e-safety related issues that arise, to the E-Safety Co-ordinator • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack, e.g. keeping virus protection up-to-date • To ensure the security of the school ICT system • To ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices • The school's policy on web-filtering is applied and updated on a regular basis • JSPC is informed of issues relating to filtering • That he/she keeps up-to-date with the school's E-Safety policy and technical information in order to effectively carry out their ESafety role and to inform and update others as relevant • That the use of the network/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety Co-ordinator/Headteacher for investigation/action/sanction • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities

	• To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities, if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content, such as copyright laws
All staff	• To read, understand and help promote the school's E-Safety policy and guidance • To read, understand, sign and adhere to the school staff Acceptable Use/Agreement/Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the E-Safety Coordinator • To maintain an awareness of current e-safety issues and guidance, e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones, etc.
Pupils	• Read, understand, sign and adhere to the Student/Pupil Acceptable Use policy (note: at KS1, it would be expected that parents/carers would sign on behalf of the pupils) • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To know and understand school policy on the use of mobile phones, digital cameras and handheld devices • To know and understand school policy on the taking/use of images and on cyber bullying • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home • To help the school in the creation/review of E-Safety policies • Logon only with their own username (Year 2 and above) • Know how to keep their personal information and passwords safe and private
Parents/ Carers	• To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement, which includes the pupils' use of the internet and the school's use of photographic and video images • To read, understand and promote the school Pupil Acceptable Use Agreement with their children • To access the school website and use social media in accordance with the relevant school Acceptable Use Agreement • To consult with the school if they have any concerns about their children's use of technology
External Groups	• Any external individual/organisation will sign an Acceptable Use policy prior to using any equipment or the internet within school

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff
- Acceptable Use Agreements discussed with pupils at the start of each year
- Acceptable Use Agreements to be issued to whole school community, usually on entry to the school
- Acceptable Use Agreements to be held in pupil and personnel files

Handling complaints:

- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

– interview/counselling by class teacher/Head of Key Stage/E-Safety Coordinator/Headteacher;
– informing parents or carers;
– removal of internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework;
– referral to LA/police.

- Our E-Safety Co-ordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyber bullying are dealt with in accordance with our Anti-Bullying policy. Complaints related to child protection are dealt with in accordance with school/LA safeguarding procedures.

Version control

As part of the maintenance involved with ensuring your E-Safety policy is updated, revisions will be made to the document. It is important that the document owner ensures the document contains the following information and that all revisions are stored centrally for audit purposes.

2. Education and curriculum

Pupil E-Safety curriculum

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach.

The education of students / pupils in online safety is therefore an essential part of the school's / academy's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities

This school

• has a clear, progressive e-safety education programme as part of the computing curriculum/PSHE curriculum. It is built on LA e-Safeguarding and e-Literacy framework for EYFS to Year 6/national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:

– to STOP and THINK before they CLICK or Zip it, Block it, Flag it;
– to develop a range of strategies to evaluate and verify information before accepting its accuracy;
– to be aware that the author of a website/page may have a particular bias or purpose and to develop skills to recognise what that may be;
– to know how to narrow down or refine a search;
– [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
– to understand acceptable behaviour when using an online environment email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
– to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
– to understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments;
– to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
– to understand why they must not post pictures or videos of others without their permission;
– to know not to download any files, such as music files, without permission;
– to have strategies for dealing with receipt of inappropriate materials;
– [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
– to understand the impact of cyber bullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
– to know even when deleted, things written online/social media are permanent.

To know how to report any abuse including cyber bullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or NSPCC.

• plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
• will remind students about their responsibilities through an end-user Acceptable Use policy, which every student will sign;
• ensures staff will model safe and responsible behaviour in their own use of technology during lessons;
• ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
• ensures that staff and pupils understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include risks in pop-ups; buying online; online gaming/gambling.
• keep staff up to date with information that they obtain on latest scams, phishing emails or social media issues.

Staff and Governor training

It is essential that all Governors and staff receive online safety training and understand their responsibilities, as outlined in this policy.

This school

• ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data;
• makes regular training available to staff on e-safety issues and the school's e-safety education program; annual updates/termly staff meetings etc.
• provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the E-Safety policy and the school's Acceptable Use policies.
• This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.

Parent awareness and training

Many parents and carers have only a limited understanding of online 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 inappropriate material on the internet and may be unsure about how to respond.

This school

• runs a rolling programme of advice, guidance and training for parents, including:

– introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear;
– information leaflets; in school newsletters; on the school website;
– demonstrations, practical sessions held at school;
– suggestions for safe internet use at home;
– provision of information about national support sites for parents e.g. www.saferinternet.org.uk/http://www.childnet.com/parents-and-carers (see appendix for further links / resources).

3. Expected conduct and incident management

Expected conduct

In this school, all users:

• are responsible for using the school ICT systems in accordance with the relevant Acceptable Use policy, which they will be expected to sign before being given access to school systems. At KS1, it would be expected that parents/carers would sign on behalf of the pupils;
• need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences;
• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;

- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety policy covers their actions out of school, if related to their membership of the school;
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking/use of images and on cyber bullying.

Staff:

- are responsible for reading the school's E-Safety policy and using the school ICT systems accordingly, including the use of mobile phones, and handheld devices;
- must only use Office 365 One Drive to store and transport data, unless they have express permission from the Headteacher/Deputy Headteacher to use an encrypted memory stick;
- must report any lost memory sticks, I-pads or laptops, within 24 hours of losing them, to SLT, so that they can inform the Data Protection Officer and ICO within 72 hours of its loss.

Students/Pupils:

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers:

- should provide consent for pupils to use the internet, as well as other technologies, as part of the E-Safety Acceptable Use Agreement form at time of their child's entry to the school;
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Unsuitable / inappropriate activities

Some internet activity, e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities, e.g. cyber-bullying would be banned and could lead to criminal prosecution.

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

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

USER ACTIONS		ACCEPTABLE	ACCEPTABLE AT CERTAIN TIMES	ACCEPTABLE FOR NOMINATED	UNACCEPTABLE	UNACCEPTABLE AND ILLEGAL
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks	Child sexual 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 the UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) – contrary to the Public Order Act 1986					X
	Pornography				X	X
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				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, website or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	X
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	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	
Online gaming (educational)			X			

Online gaming (non-educational)			X	X	
Online gambling				X	
Online shopping/commerce			X		
File Sharing			X		
Use of Social Media				X	
Use of Messaging Apps			X		
Use of video broadcasting e.g. YouTube			X		

In this school:

- there is strict monitoring and application of the E-Safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions;
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported;
- support is actively sought from other agencies as needed (e.g. the local authority, police and UK Safer Internet Centre helpline) in dealing with e-safety issues;
- monitoring is conducted visually by staff and through the e-safe monitoring software;
- monitoring and reporting of e-safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, governors/the LA/LSCB;
- parents/carers are specifically informed of e-safety incidents involving young people for whom they are responsible;
- we will contact the police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

  - Internal response or discipline procedures
  - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
  - Police involvement and/or action

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:

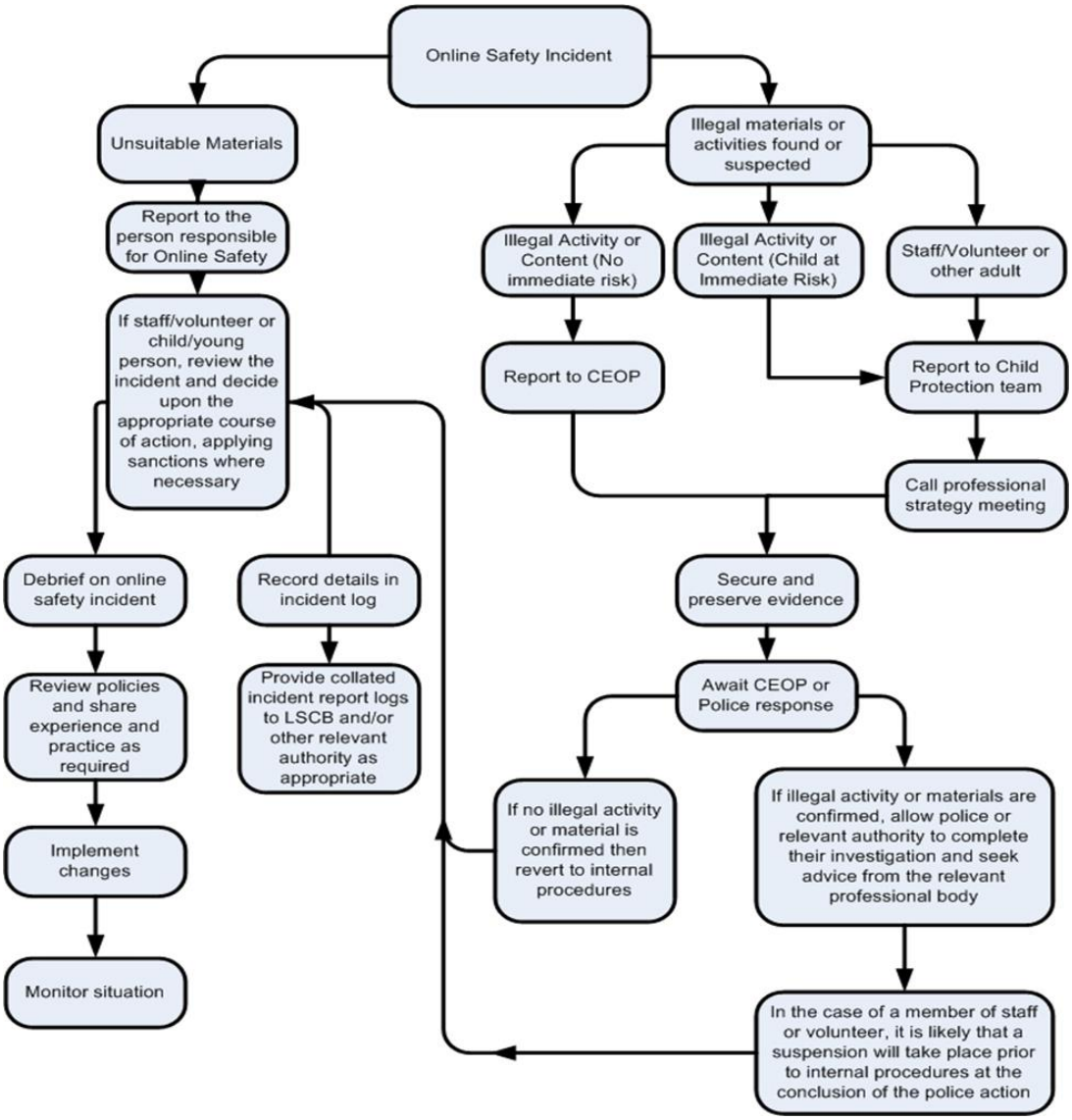
o incidents of 'grooming' behaviour
o the sending of obscene materials to a child
o adult material which potentially breaches the Obscene Publications Act
o criminally racist material
o promotion of terrorism or extremism
o other criminal conduct, activity or materials

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

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Illegal Incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Actions and Sanctions

	Actions / Sanctions								
Students / Pupils Incidents	Refer to class teacher	Refer to Phase Leader	Refer to ESafety Co-ordinator/Headteacher	Refer to Police	Refer to technical support staff (JSPC) for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg miss break time / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X	X	X			X	X	X	
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	X	X	X			X	X	X	X
Unauthorised / inappropriate use of social media / messaging apps / personal email	X	X	X		X	X	X	X	X
Unauthorised downloading or uploading of files	X	X	X		X			X	
Attempting to access or accessing the school network, using another pupil's account	X	X	X			X	X	X	
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X			X	X	X	
Corrupting or destroying the data of other users	X	X	X			X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X		X	X	X	X
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school	X	X	X	X		X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X	X	X	X	X	X	X	X

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

Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X			X	X		X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X
Loss of data via memory stick which has been reported to SLT		X	X	X				
Loss of data not reported		X	X	X		X	X	X

4. Managing the ICT infrastructure

Internet access, security (virus protection) and filtering

This school:

- has the educational filtered secure broadband connectivity through Exa.
- uses the Surfprotect filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- ensures network healthy through use of ESet anti-virus software etc. and network set-up so staff and pupils cannot run executable files;
- uses DfE, LA or WSSS approved systems such as S2S, secured email to send personal data over the internet and uses encrypted devices or secure 2-step authentication remote access were staff need to access personal level data off-site;
- blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- only unblocks other external social networking sites for specific purposes/internet Literacy lessons;
- has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- works in partnership with JSPC to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- requires staff to preview websites before use [where not previously viewed or cached]; plans the curriculum context for internet use to match pupils' ability, using child-friendly search engines where more open internet searching is required; e.g. kidrex.org.uk:

  - Never allows/is vigilant when conducting 'raw' image search with pupils, e.g. Google image search;
  - Informs all users that internet use is monitored;
  - Informs staff and students that that they must report any failure of the filtering systems directly to the E-Safety Co-ordinator. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or JSPC Helpdesk as necessary;
  - Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;

- Provides advice and information on reporting offensive materials, abuse/bullying etc. available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities, police and the LA.

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Has additional local network auditing software installed on admin and teaching machings;
- Ensures the Systems Administrator/E-Safety Co-ordinator is up to date with WSSS services and policies/requires the Technical Support Provider (JSPC) to be up to date with West Sussex services and policies;
- Storage of all data within the school will conform to the UK data protection requirements.

Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's E-Safety policy. Following this, they are set-up with internet, email access and network access. Online access to service is through a unique, audited username and password. We also use the same username and password for access to our school's network;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- Makes clear that no one should logon as another user and makes clear that pupils should never be allowed to logon or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has setup the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then logon again as themselves. Users needing access to secure data are timed out after a given time and have to re-enter their username and password to re-enter the network;
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day;
- A shutdown system is set up so all ICT Suite and Learning Street computers are logged off between 4.00pm and 4.30pm daily.
- Has setup the network so that users cannot download executable files/programmes;
- Only staff have access to music/media download or shopping sites.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs;
- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by site manager; equipment installed and checked by approved suppliers/LA electrical engineers;

- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role; e.g. teachers access report writing module; SEN Co-ordinator - SEN data;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school/LA approved systems: e.g. teachers access their area/a staff shared area for planning documentation via a VPN solution;
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support; our Education Welfare Officers accessing attendance data on specific children;
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses our broadband network for our CCTV system and have had set-up by approved partners;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange;
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level/appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

Passwords policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private;
- We require staff to use STRONG passwords for access into our MIS system;
- We require staff to change their passwords into the MIS and other secure systems every 90 days.

Email

This school

- Provides staff with an Office 365 email account for their professional use, and makes clear personal email should be through a separate account;
- Will contact the police if one of our staff or pupils receives an email that we consider is particularly disturbing or breaks the law;
- Will ensure that email accounts are maintained and up-to-date;
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the police;
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus product ESet, plus direct email filtering for viruses, trojans, pornography, phishing and inappropriate language. Finally, and in support of these, Surfprotect Filtering monitors and protects our internet access to the World Wide Web.

Pupils

- We use Surfprotect for pupils and lock this down where appropriate using Surfprotect rules.
- Pupils are introduced to, and use email as part of the ICT/Computing scheme of work.
- Pupils are taught about the safety and 'netiquette' of using email both in school and at home, i.e. they are taught:

  - not to give out their email address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
  - that an email is a form of publishing where the message should be clear, short and concise;
  - that any email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
  - they must not reveal private details of themselves or others in email, such as address, telephone number etc.;
  - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
  - that they should think carefully before sending any attachments;
  - embedding adverts is not allowed;
  - that they must immediately tell a teacher/responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature;
  - not to respond to malicious or threatening messages;
  - not to delete malicious of threatening emails, but to keep them as evidence of bullying;
  - not to arrange to meet anyone they meet through email without having discussed with an adult and taking a responsible adult with them;
  - that forwarding 'chain' email letters is not permitted.

- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including email and we explain how any inappropriate use will be dealt with.

Staff

- Staff can only use the Office 365 email systems on the school system.
- Staff only use Office 365 email systems for professional purposes.
- Access in school to external personal e mail accounts may be blocked.
- Never use email to transfer staff or pupil personal data. We use secure, LA/DfE approved systems. These include: S2S (for school to school transfer); Collect.
- Staff know that email sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':

  - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
  - the sending of chain letters is not permitted;
  - embedding adverts is not allowed.

- Staff are asked to use the Office 365 One Drive cloud storage to work on data away from school.
- All staff sign our LA/School Agreement Form AUP to say they have read and understood the e-safety rules, including email and we explain how any inappropriate use will be dealt with.

School Website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- Our Website Co-ordinator keeps the website up to date.
- The Website Governor monitors the content to ensure that it is compliant with statutory requirement.
- Uploading of information is restricted to our website authorisers, e.g. administration officer.
- The school website complies with the statutory DfE guidelines for publications.
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the website is the school address, telephone number and we use a general email contact address, e.g. office@Estcotspri.co.uk. Home information or individual email identities will not be published.
- Photographs published on the web do not have full names attached.
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.
- We do not use embedded geodata in respect of stored images.
- We expect teachers using school approved blogs or wikis to password protect them and run from the school website.

Social Networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- The school's preferred system for social networking will be maintained in adherence with the communications policy.
- School staff will ensure that in private use:
- 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.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (retained by the Support Provider for 28 days), without permission except where disclosed to the police as part of a criminal investigation.

5. Data Security: Management Information System access and Data Transfer

Strategic and Operational Practices

At this school:

- The Headteacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (The Headteacher). We ensure that staff know who to report to regarding any incidents where data protection may have been compromised.

- All staff are DBS-checked and records are held in one central record in SIMS.
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed:

  - staff
  - governors
  - pupils
  - parents

This makes clear staffs' responsibilities with regard to data security, passwords and access.

- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services/Family Services, Health, Welfare and Social Services.
- We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home. This has a 2-step authentication logon.
- School staff with access to setting-up usernames and passwords for email, network access and CPOMS access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual housekeeping to review, remove and destroy any digital materials and documents which need no longer be stored.
- Staff are made fully aware of the need to report any loss of equipment containing data to SLT and the consequences if this is not done.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to logout of systems when leaving their computer.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the DfE S2S Admissions system to transfer admissions data.
- We use a secure VPN solution for remote access into our systems.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any back-up tapes in a secure, fireproof safe. No back-up tapes leave the site on mobile devices.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded.

6. Equipment and digital content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's and parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.

- Student mobile phones which are brought into school must be turned off (not placed on silent) and stored with the Reception Office on arrival at school. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during school break times. All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or handheld devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the school's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call, they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the written prior consent of the person or people concerned.

Students' use of personal devices

- The School strongly advises that student mobile phones should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into lessons.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.

Staff use of personal devices

- Any permitted images or files taken in school must be downloaded from the device and deleted as soon as possible.
- Staff are not advised to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity, unless there are exceptional circumstances, which have been agreed by a member of the senior leadership team.

- Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose. If a member of staff breaches the school policy, then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during offsite activities, or for contacting students or parents, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes. Wherever possible, staff should contact the School Office, who will then contact parents or use the school mobile.

Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences, which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information;
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2013. Further information can be found on the Environment Agency website.

Estcots Primary School
Pupil Acceptable Use Policy

All pupils must follow the rules in this policy when using school computers, and the school Moodle.

Pupils that do not follow these rules may find:

- they are not allowed to use the computers,
- they can only use the computers if they are more closely watched.

Their teachers will show pupils how to use the computers.

Computer Rules	
1	I will only use polite language when using the computers.
2	I must not write anything that might: upset someone or give the school a bad name.
3	I know that my teacher will regularly check what I have done on the school computers.
4	I know that if my teacher thinks I may have been breaking the rules they will check on how I have used the computers before.
5	I must not tell anyone my name, where I live, or my telephone number - over the Internet.
6	I must not tell my username and passwords to anyone else but my parents.
7	I must never use other people's usernames and passwords or computers left logged in by them.
8	If I think someone has learned my password then I will tell my teacher.
9	I must log off after I have finished with my computer.
10	I know that e-mail is not guaranteed to be private. I must not send unnamed e-mails.
11	I must not use the computers in any way that stops other people using them.
12	I will report any websites that make me feel uncomfortable to my teacher/a member of staff.
13	I will tell my teacher/a member of staff straight away if I am sent any messages that make me feel uncomfortable.
14	I will not try to harm any equipment or the work of another person on a computer.
15	If I find something that I think I should not be able to see, I must tell my teacher straight away and not show it to other pupils.

UNACCEPTABLE USE

Examples of unacceptable use include, but are not limited to:

- Using a computer with another person's username and password.
- Creating or sending on the Internet any messages that might upset other people.
- Looking at, or changing work that belongs to other people.

- Waste time or resources on school computers.

Student User Agreement Form for the Student Acceptable Use Policy

I agree to follow the school rules when using the school computers. I will use the network in a sensible way and follow all the rules explained by my teacher.

I agree to report anyone not using the computers sensibly to my teacher.

I also agree to tell my teacher or another member of staff, if I see any websites that that make me feel unhappy or uncomfortable.

If I do not follow the rules, I understand that this may mean I might not be able to use the computers.

Student Name: .....

As the parent/legal guardian* of the pupil named above, I give permission for my child to access networked computer services such as the Internet, e-mail and the schools Virtual Learning Environment (such as Moodle).
I understand that pupils will be held accountable for their own actions.

I also understand that although the school will take reasonable steps to ensure that my child is appropriately supervised, according to age and responsibility, I will not hold the school or County Council responsible for inappropriate material that my child may obtain.

I understand the school reserves the right to apply monitoring arrangements to any student in relation to network, e-mail and Internet use where misuse is suspected. I accept responsibility for setting standards for my son or daughter to follow when selecting, sharing and exploring information and media. I agree to report any misuse of the network to the school.
Please circle appropriate boxes below (Yes or No)

• My child's work, if selected, ***may*** be published on the Internet, including the school and West Sussex County Council websites	Yes	No
• My child ***may*** take part in Internet / video conferencing between the school and another institution	Yes	No

Parent/Carer/Guardian's Name: ..... Date: .....

Parent/Carer/Guardian's Signature: .....

Estcots Primary School
Staff Acceptable Use Policy

School networked resources, including the internet, are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. If you make a comment about the school or county Council, you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the school or County Council into disrepute is not allowed.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to the withdrawal of the user's access, monitoring and/or retrospective investigation of the Users' use of services and, in some instances, could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

CONDITIONS OF USE

Personal Responsibility

Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to the Headteacher.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Below is a list of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the Estcots Code of Conduct.

1	I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school (or West Sussex County Council) into disrepute.
2	I will use appropriate language – I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3	I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4	I understand that if staff are under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.
5	Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) or other users to any unauthorised person (see 21). I will not reveal any of my personal information to students.
6	I will not trespass into other Users' files or folders.
7	I will ensure that all my login credentials (including passwords) are not share with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other Users.
8	I will ensure that, if I think someone has learned my password, I will change it immediately and contact the Headteacher.
9	I will ensure that I log off after my network session has finished.

10	If I find an unattended machine logged on under another User's username, I will not continue using the machine – I will log it off immediately.
11	I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the school leadership team.
12	I am aware that email is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
13	I will only use the Office 365 email system on the school network.
14	I will not use emails other than Office 365 to transfer staff or pupil personal data.
15	I will not use the network in any way that would disrupt use of the network by others.
16	I will report any accidental access, receipt of inappropriate materials or filtering breaches/unsuitable websites to the Headteacher.
17	I will not use USB drives, portable hard drives, or personal laptops on the network without having them encrypted and approved by SLT and JSPC and checked for viruses.
18	I will not attempt to visit websites that might not be considered appropriate or are illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
19	I will not download any unapproved software, system utilities or resources from the internet that might compromise the network or are not adequately licensed.
20	I will not accept invitations from children and young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine. As damage to professional reputations can inadvertently be caused by quite innocent postings or images, I will also be careful with who has access to my pages through friends and friends of friends; especially with those connected with my professional duties, such as school parents and their children.
21	I will ensure that any private social networking sites/blogs etc. that I create, or actively contribute to, are not confused with my professional role in any way.
22	I will support and promote the school's E-Safety and Data Security policies and help students be safe and responsible in their use of the internet and related technologies.
23	I will not send or publish materials that violate the Data Protection Act or breach the security this Act requires for personal data, including data held on the SIMS Learning Gateway.
24	I will not receive, send or publish material that violates the copyright law. This includes materials sent/received using video conferencing or web broadcasting.
25	I will not attempt to harm or destroy any equipment or data or another User or network connected to the school system.
26	I will ensure that portable ICT equipment such as laptops, digital still, I-pads and video cameras are securely locked away when not being used.
27	I will ensure that any personal data (where the Data Protection Act applies), that is sent over the internet, will be encrypted or otherwise secured.
28	I will not add APPs to the school system without the permission of the Headteacher.
29	If I lose any storage device containing data, I will report it to the SLT Within 24 hours, so that it can be reported to the Data Protection Officer and the ICO.

Additional Guidelines

- Staff must comply with the Acceptable Use Policy of any other networks that they access.
- Staff will follow the 'Safer Use of the Internet by Staff working with Young People' published with the West Sussex Schools Acceptable Use Policy – https://SWGfl.org.uk

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries or service interruptions caused by the system or your errors of optimism. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY

Users are expected to inform the Headteacher immediately if a security problem is identified and should not demonstrate this problem to other Users. Files held on the school's network will be regularly checked by the Headteacher. Users identified as a security risk will be denied access to the network.

MEDIA PUBLICATIONS

Written permission, from parents or carers, must be obtained before photographs of, or named photographs of students, are published. Also, examples of students' work must only be published (e.g. photographs, videos, TV presentations, web pages etc.) if written parental consent has been given.

Staff User Agreement Form for the Staff Acceptable Use Policy

As a school User of the network resources, I agree to follow the school rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the school Acceptable Use Policy. If I am in any doubt, I will consult the Headteacher.

- I agree to report any misuse to the Headteacher.
- I also agree to report any websites that are available on the school internet that contain inappropriate material to the Headteacher/E-Safety Co-ordinator.
- Lastly, I agree to ensure that portable equipment, such as cameras, I-pads or laptops will be kept secured when not in use, and to report any lapses in physical security to the Headteacher within 24 hours.
- If I do not follow the rules, I understand this may result in the loss of access to these resources, as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse, in terms of time or content, may be placed under retrospective investigation, or have their usage monitored.

Staff name: .....

Signature: .....

Date: .....