Holy Trinity Rosehill VA CE Primary School

E-Learning Policy

(Including Computing, ICT, E-Safety, Social Media, Internet, Acceptable Use and Digital Technologies)

Holy Trinity Rosehill C.E. (VA) Primary School
E-Learning Policy

This policy should be read in conjunction with other school policies including Anti-Bullying, Behaviour, PSHE, Child Protection, Data Protection, Copyright Protection and Freedom of Information policies.

Introduction

This policy aims to cover the different elements that E-Learning can cover within our school. These guidelines have been created to ensure that all stakeholders within the school are aware of what is expected of them and are able to stay safe when using the hardware and software we have in school. The equipment and resources within school are provided to enhance the learning of the pupils and to aid the staff in their delivery of the curriculum; this policy will enable these happen. Holy Trinity Rosehill recognises that its pupils are entitled to quality hardware and software and a structured and progressive approach to the learning of the skills needed to enable them to use it effectively. We recognise that E-Learning is more than a matter of 'information technology' and use the term E-Learning as the over-arching theme to describe:

- **Computing** – the statutory curriculum subject as set out in the National Curriculum (2014) which includes the strands of:
  - Digital Literacy
  - Computer Science
  - Information Technology
- **Information Communications Technology (ICT)** – the ways in which we embed digital technologies across the curriculum to support and extend children's learning.

This policy will also set out a framework for how Computing will be taught, assessed and monitored throughout the school and should reflect the ethos and philosophy of our school. It will also highlight how ICT can be used across the curriculum. This policy has been written with guidance and support from other teachers, schools and local authorities and aims to meet the criteria established by organisations such as Becta, 360Safe and ICT Mark. Often schools will have a number of policies including E-safety and Social Media, but as a school we have decided to combine them into one policy. Further information on the different systems in school will be made available to staff online through the school's website and the htrschool.net learning environment.

Rationale

Technologies encompass every part of modern life and it is important that our children are taught how to use these tools and more importantly, how to use them safely. We believe that it is important for children, staff and the wider school community to have the confidence and ability to use these tools to prepare them for an ever-changing and rapidly developing world. To enable all our staff and pupils to be confident, competent independent users and learners of digital technologies we aim:

- To use digital technologies where appropriate to ensure pupils are motivated and inspired in all areas of the curriculum
- To use digital technologies to help improve standards in all subjects across the curriculum
- To develop the digital technologies competencies and skills of pupils through computing lessons and provide them with the chance to consolidate these in a cross-curricular context
- To ensure pupils are challenged in their use of digital technologies and are provided with exciting, creative ways in which to share their learning
- To use tools available to ensure children have the ability to work independently and collaboratively to suit the needs of the situation
- To provide all staff with the training and support to ensure that they can, and have the confidence to, use digital technologies, ICT and Computing to its full potential in all aspects of school life
- To use digital technologies as a form of communication with parents, pupils and the wider community

Aims

The school's aims are to:

- provide a relevant, challenging and enjoyable curriculum for e-learning for all children.
- meet the requirements of the National Curriculum Programmes of Study for Computing.
- use digital technologies as a means to enhance learning throughout the curriculum
- respond to new developments in technology.

Organisation

The school believes that progress in E-Learning is promoted through regular access and use of technology relevant to a task.

- The predominant mode of working with digital technologies is as individuals or in small groups.
- New skills may be introduced to a group of pupils.
- Practice of skills will occur discretely while using ICT to support work across the curriculum.

1. Computing Curriculum

Computing will be taught as a discrete curriculum subject according to the guidance in the National Curriculum for KS1 and KS2. There will be a need for the pupils to be taught stand-alone computing lessons but opportunities for developing computing across the curriculum should also be developed. The computing curriculum is split into three areas:

1. Digital Literacy
2. Computer Science
3. Information Technology

Teachers in KS1 and KS2 follow guidance and units of work from the 'Switched on Computing' scheme of work which provides full coverage of the National Curriculum objectives for KS1 and KS2. The long term map shows the journey the pupils are expected to take from Years 1 to Year 6.

In the Early Years (Nursery and Reception), staff follow the guidance of the 'Switched on ICT: Early Years' scheme of work which allows the children to be taught how to use various digital technologies and equipment, including computer, iPads and cameras in accordance to the Early Learning Goals appropriate for them.

The E-Learning Coordinator and Shadow E-Learning Coordinator will ensure that the plans provide coverage of what is expected through the new National Curriculum and Early Learning Goals. They will also ensure that the children are challenged and are able to succeed.

Opportunities for ICT across the curriculum should also be promoted at all levels across the school. Digital technologies are fundamental to children's learning in our society they should be used when relevant in all curriculum subjects.

1.1. Planning, assessment, recording and reporting of Computing

- Computing skills will be assessed and taught using the schools own Switched on Computing scheme of work in KS1 and KS2 and the STEPS system in Early Years.
- New skills may be taught discreetly during computing time to enable pupils to achieve stated objectives and then applied during work across the curriculum to consolidate their learning.
- Pupil progress towards these objectives will be recorded by teachers as part of their class recording system
- Pupils will save work on the school network. Other work may be printed and filed within the subject from which the task was set.
- Progress in computing will be reported upon in the pupil's annual report

1.2. Planning of Computing

Breadth of experience in Computing education will be achieved by offering children the opportunity to gain access to ICT across a range of contexts building upon the child's previous understanding and knowledge.

Balance of experience will be achieved, as every opportunity will be given to every child to gain experience in each strand. It is intended that all strands of the Computing National Curriculum should be covered within a Key Stage by careful planning into curriculum topics. Teachers will assess each child's progress half termly using the 'Switched on Computing' guidelines.

1.3. Teaching of Computing

Teachers are encouraged to use a variety of teaching styles in order to introduce new programmes and skills. Children are given the opportunity to work in small groups, pairs, individually and as a whole class. It should be noted that different groupings are flexible to ensure equal opportunities and that appropriate differentiation is maintained at all times to meet the needs of individual children.

At Holy Trinity Rosehill, we believe that computing must be presented in practical contexts, which will be relevant to the children's experiences; pupils must have "hands on" experience. Computers are located in 2 ICT suites with programs available that are appropriate to the differing age range and abilities within the school. The School's Computing Scheme of Work contains full details of the learning stages of ICT, the programs to be used and the skills that need to be developed in each year group. **Not all Computing learning will involve the use of computers.**

1.4. Pupil Objectives for Computing

Learning with ICT at the Foundation Stage
Young children should begin to show an interest in ICT. During the Foundation Stage, children should have opportunities to find out about and identify the uses of everyday technology and use ICT and programmable toys to support their learning.
Children with special educational needs and/or disabilities need to be provided with access to appropriate resources. Staff in the Early Years follow the 'Switched on Early Years' scheme of work in order to meet the Early Learning Goals.

The Early Learning Goal relating to technology states:

- Children recognise that a range of technology is used in places such as homes and schools. They select and use technology for particular purposes.

In addition, Foundation Staff also follow a progression through the STEPS system and assess children according to their understanding:

- D (22-36 months) - Operates mechanical toys.
- D (22-36 months) - Seeks to acquire basic skills in turning on and operating some ICT.
- E (30-50 months) - Knows that information can be retrieved from computers.
- E (30-50 months) - Shows skill in making toys work by pressing parts or lifting flaps to achieve effects such as sound, movements or new images.
- E (30-50 months) - Knows how to operate simple equipment.
- E (30-50 months) - Shows an interest in technological toys with knobs or pulleys, or real objects.
- F (40-60 months) - Completes a simple program on a computer.
- F (40-60 months) - Uses ICT hardware to interact with age-appropriate computer software.

The school follows the statutory National Curriculum for Computing. These statutory objectives relate to Key Stages 1 and 2.

At the end of KS1 children should:

- understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following precise and unambiguous instructions
- create and debug simple programs
- use logical reasoning to predict the behaviour of simple programs
- use technology purposefully to create, organise, store, manipulate and retrieve digital content
- recognise common uses of information technology beyond school
- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

At the end of KS2 children should:

- design, write and debug programs that accomplish specific goals, including controlling or simulating physical systems; solve problems by decomposing them into smaller parts
- use sequence, selection, and repetition in programs; work with variables and various forms of input and output
- use logical reasoning to explain how some simple algorithms work and to detect and correct errors in algorithms and programs
- understand computer networks, including the internet; how they can provide multiple services, such as the World Wide Web, and the opportunities they offer for communication and collaboration
- use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and

content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information

- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact

As a school we follow the 'Switched on ICT in the Early Years' and 'Switched on Computing' scheme of work.

2.5. Recording, Assessment and Reporting

Computing will be assessed in a number of ways using formative and summative assessment. Formative assessment will happen during Computing lessons and will be used to inform future planning and this is conducted by the teacher on an informal basis. Computing capability will be completed on a termly basis with notes being taken by the teacher and this will link to 'Switched On' schemes of work in Early Years, KS1 and KS2.

Staff in Early Years will use the Early Learning Goals and STEPS system to assessment the children's understanding and use of digital technologies at the end of the Foundation Stage.

2. Internet, Systems and Services

Access and Deployment

IT network infrastructure and equipment has been sited so that;

- Each classroom has a computer connected to the network and an Interactive Whiteboard.
- There is are computer suites in both the EYFS/KS1 and KS2 departments; classes can work in pairs during whole class ICT time.
- Nursery and Reception also have desktop computers in the classrooms.
- Other equipment such as digital cameras and iPads are available from shared bank for classes to use.

Online Learning

As a school, we value the importance of providing opportunities for children to learn outside of school and we will provide these depending on the age of the child.

Through our htrschool.net learning platform, for children in Reception, Key Stage 1 and Key Stage 2 we will:

- Provide logins for htrschool.net and the *Pupil Learning Hub* which includes our Google Apps for Education Environment which includes tools such as email and website creation.
- Logins for online tools such as Purple Mash, Espresso Primary and Education City.
- Access, with moderated posting rights, to their class blog.

Resources

The school acknowledges the need to continually maintain, update and develop its digital resources and to make progress towards a consistent, compatible IT system by:

- Maintaining a computer system to deliver a relevant and diverse curriculum
- Investing in software and hardware that will effectively deliver the strands of the Computing curriculum
- Investing in software that will support the use of ICT across the curriculum

Investing in infrastructure and equipment to improve children's access to ICT across the curriculum and which also keep up to date with latest developments in technology.

Resource Management

Holy Trinity Rosehill is committed to reviewing the position and use of digital resources. The school will ensure the efficient deployment of existing digital resources and develop strategies for their replacement and for further purchasing to meet future needs.

Equipment, Hardware and Software

Hardware should not be installed without the permission of the head teacher and/or E-Learning Leader. If staff intend to use memory sticks which include sensitive information including (and not limited to) children's names then they must use an encrypted memory stick that has been provided by school. If staff use memory sticks to store other non-sensitive data then the school's antivirus software will scan these. Staff should be vigilant to reduce the risks of virus infection as stated in the AUP.

The installation of software unauthorised by the school, whether licensed or not, is forbidden. If you are unsure, please speak to the head teacher and/or the E-Learning leader for advice. The school reserves the right to examine or delete any files that are held on its system.

Teaching staff are provided with a laptop computer for the purposes of planning, preparation and assessment and these should be used within this remit. The laptop computers remain the properly of the school and should be returned upon request. To use the internet at home, staff will need to change the internet settings as required. Antivirus, firewall and other management software must not be uninstalled.

Network

Staff will be issued with a username for the computer system and a simple password. It is their responsibility to change this in accordance with the password procedure below.

Pupils in Reception will not be expected to log on to the network and this may be done for them. From Year 1, children are expected to use their own individual logins for the system.

There are three categories of user on the system: pupils, admin and staff. Each level is managed by ONE ITSS who provide the support and infrastructure for our computer system.

The school has a MANAGED wireless network. There are two levels of access for this network – "full access" and "guest access". The "full access" password is managed by ONE ITSS and should only be available to the Head Teacher, E-Learning Leader and Shadow E-Learning Coordinator. All school owned equipment is placed on the "full access" network. The "guest network" allows users to access filtered internet without connecting to our computer system. The password for this is available for staff and visitors on request. Staff and visitors may connect their own devices to this network. If the password is provided on paper, it should be destroyed once it has been used. Further information about staff and pupil use is included in the acceptable use policies.

Backups

Every school day the main server is set to backup essential files and settings. This is undertaken by ONE ITSS as part of their service level agreement.

Security

- All ICT equipment will be security marked and noted in the school inventory
- Any equipment taken off site should be signed out using the log book in the main office.
- The ICT Technician will be responsible for regularly updating anti-virus software
- No discs from outside school should be allowed in machines without permission from the E-Learning Leader.
- Use of ICT will be strictly in line with the school's 'Acceptable Use Policy for Staff'
- Parents/carers will be made aware of the 'Acceptable Use policy for Children' and will be asked to counter-sign this with their child.
- All pupils and parents will be aware of the School Rules for Responsible Use of ICT and the Internet and will understand the consequence of any misuse.
- The agreed rules for Safe and Responsible Use of ICT and the Internet will be displayed in all ICT areas.

htrschool.net including school website and blogs

(Linked to 360Safe Public Facing and Professional Standards Guidelines)

Our school has a dedicated Wordpress network installation which hosts our htrschool.net online platform, school website and blogs. The school website is overseen by the E-Learning Leader with the support of the Shadow E-Learning Leader and it is expected that certain areas (in particular class blogs) will be added to, updated and maintained by other members of staff and children.

The htrschool.net is managed and hosted by Renoovo Design who provide the technical support and development of the system. They are also responsible for the backup and maintenance of our system through a service level agreement.

The htrschool.net system also includes features from Google Apps for Education. This is a free system that contains a number of tools including email, document sharing and website creation. All children in Reception to Year 6 are given a login and are given permission to use different tools according to their age and e-safety awareness. Children may need to prove that they can use tools safely before having them enabled. The Google Apps for Education service is managed by the E-Learning Leader with the support of the Shadow E-Learning Coordinator. Google stores data about its users in accordance with the Safe Harbour Agreement approved by Becta before its closure in 2011.

Internet and E-mail

The internet may be accessed by staff and by children throughout their hours in school. Filtering is provided as part of our service level agreement with ONE ITSS and different levels of filtering are activated for staff and pupils. The guest network as part of our wireless network has a high level of filtering enabled.

The teaching of email and internet should be covered within the Computing curriculum planning, but staff should encourage regular dialogue that explores the benefits and potential dangers of using the internet.

All staff and governors will be issues with a school email address and this is the email with which they should use for professional communication. Staff use the sbcschools.org.uk email system which is provided as part of our service level agreement with ONE ITTS. Govenors use the htrschool.net email system. Further information about acceptable use can be found the acceptable use area of this policy.

As part of their access to the htrschool.net system, children will also be issued with an email address. This email address is part of the Google Apps for Education service and has the following access levels:

- Early Years – No email access (email address is used as username)
- KS1 – Internal messaging only.
- KS2 – Internal and external messaging.

The email service provides children with a @htrschool.net email address and within this system all incoming and outgoing emails are logged under a separate account (reporting@htrschool.net). We also have strict filtering system in place which scans for profanities and inappropriate language. Should an email trigger our filter then the email is blocked and reported to the Head Teacher and E-Learning Leader.

Staff should take extra care to ensure that all communication with children and/or parents remains professional. Users are responsible for all messages that are sent and due regard should be paid to the content of the emails to ensure it is not misconstrued. All web activity is monitored by ONE ITSS so it is the user's responsibility to ensure they log off appropriately. If children receive an email that they believe to be inappropriate then they should forward it on to their teacher and/or the E-Learning Leader who will investigate.

The use of the internet to access inappropriate materials such as auction sites, pornography, racist or any other material is prohibited. If users, especially children, do see an inappropriate website or image, they should close this immediately and report the site to the class teacher who should then report it to ONE ITSS and the E-Learning Leader.

Zombie Accounts

Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access. We will:

- Ensure that all user accounts are disabled once the member of the school has left
- Prompt action on disabling accounts will prevent unauthorized access
- Regularly change generic passwords to avoid unauthorised access

Passwords

(Linked to 360Safe Password Guidelines)
Staff should make sure that any passwords they use are strong and contain a mixture of some of the following; upper- and lower-case letters, numbers and punctuation. These should be changed regularly, especially if the user suspects others may know the password.

Children are provided with a username and password which we aim to make generic across the computer system and online services (with the exception of some sites requiring a prefix or a different username/password). Children should be taught not to share passwords and the reason for this. If a child suspects that their password has been compromised then they should tell their class teacher who should report it to the E-Learning Leader who will then change the password.

Age Limits

Certain online tools have age limits on the use of their software. This is due to an Act of United States Law. The Children's Online Privacy Protection Act prevents websites collecting data or providing their services to users under the age of 13.

As a school, we may decide to use some of these tools within lessons but will do so after thoroughly testing them for their safety and appropriateness. We will also post details of these sites on our school webpage. We will ensure that these will tend to be sites that allow creation of content rather than searching other users' content.
Occasionally these sites will be used by teachers with a class, for example to create a class book or movie, but not by a child with their own personal account. We will make parents aware of this during our e-safety events. If they do not wish their child to access these sites, their child can be provided with an alternative method to complete the task.

Health and Safety

The school is aware of the Health and Safety issues involved in children's use of digital technologies and follows the recommendations made by Stockton Borough Council. The school will dispose of redundant ICT equipment responsibly, safely and appropriately through ONE ITSS.

Administrative Systems

- The school administration will remain separate from the curriculum system. Class teachers have access to SIMs for registration, assessment and reporting purposes with their own log in. Access to the rest of the system is only available to members of the Senior Leadership and Management Team and members of the school office.
- All staff members have a school email account through the sbcschools.org.uk email system
- All staff members have access to the htrschool.net online system

Technical Support

Most issues should be dealt with my ONE ITSS as part of our service level agreement. Issues can be logged on an online help desk which is provided by ONE ITS. Many minor issues are dealt with by the ICT Coordinator and the Digital Leaders as appropriate.

4. Social Media

(Linked to 360Safe Social Media Guidelines)

The school recognises that many staff will actively use Facebook, Twitter and other such social networking, blogging and messaging services. We also recognise that social media and networking sites are playing an increasing role within every-day life and that many staff are users of tools such as Facebook, Twitter and blogs using these for both personal and professional use. We will ensure that staff and children are kept fully aware of risks and issues that may arise and ways in which to minimise these risks. Although these networks are used by staff in their own time, staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks. Staff are encouraged to review their privacy settings to make sure that their profiles and photographs are not viewable by the general public.

It is never acceptable to accept a friendship request from a child from the school as in almost all cases children of primary age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends ex-pupils who are still minors.

Staff should:

- Ensure that their profile/posts are kept private to friends where possible, this also includes personal information such as phone numbers, email addresses etc.
- Not accept current or ex-pupils as 'friends' on social media sites such as Facebook, Instagram, Snapchap, OoVoo etc. This is to ensure any possible misinterpretation. It is never acceptable to accept a friendship request from a child from the school as in almost all cases children of primary age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends ex-pupils who are still minors. We do understand that some staff members have friends within the local community (such as children's parents) and ask that these members of staff take extra precaution when posting online.
- Ensure that if their communication is fully public (e.g. blogs/Twitter), or is visible to parents of children within the school community, that they maintain their professionalism at all times and remember that they are a representative of the school even out of school hours and at weekends.
- Be aware that electronic texts can sometimes be misinterpreted or misconstrued so should endeavour to minimise the possibility of this happening.
- Not use these media to discuss confidential information or to discuss specific children or the business of the school.
- Check with the E-Learning Leader if they need advice on monitoring their online persona and checking their security settings.

It is recognised that some such services may have an appropriate application in school, however, where such activities are planned a separate account should be set up for the purpose and there should be no connection made between personal and school accounts used for educational purposes. Any such accounts and activities should be approved by the head teacher or E-Learning Leader prior to use

Instances of online behaviour, including those on social media and the internet, which could be perceived to have a negative or detrimental impact or effect upon the reputation of the school will not be tolerated or supported by the governing body. Staff should report any instances of unacceptable online behaviour to the Head Teacher and/or Chair of Governors who will follow the staff code of conduct/school's disciplinary procedure.

Pupils should not be signed up to most social networking sites due to the over-13 age limit. However, we recognise that many are signed up either with or without parental knowledge. As a school we ensure it is part of our curriculum. We will also ensure that parents are fully aware of how to minimise the risk if their children are using these sites. As a school, we provide access to htrschool.net "Connect" which is an internal social networking site as part of our online learning environment. The aim of this is to teach the children safe practices with online social networks.

As a school we will use Twitter to post information, updates and blog posts. These will stream directly to our school website. We will ensure that we block any followers that appear inappropriate.

We use blogging throughout the school to share children's learning and to communicate with parents. We will follow guidance laid out in this document to ensure children are kept safe. No-one is able to post on the blog or write a comment without it being approved by a teacher to ensure that the children are not subjected to any inappropriate comments. Spam messages (often containing inappropriate links and language) are caught by software installed on the blog (akismet) and this is monitored by the E-Learning Leader with the support of the Shadow E-Learning Coordinator. This software is updated regularly.

Digital and Video Images

(Linked to 360Safe Digital and Video Guidelines)

Photographs and video clips add colour, life and interest to school activities and celebrate the school's achievements. We recognise that images must be used in a responsible way and we are aware of child protection issues.

The school wishes the school's web site and blogs to reflect the diversity of activities, individuals and education that can be found at Holy Trinity Rosehill C.E. (VA) Primary. From time to time the staff may take photographs and videos of children for assessment purposes and for publication on the school's blogsite etc. However, the school recognises the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when considering material for publication on the Internet, the following principles will be borne in mind:

- Surnames of children must not be published publically online;
- Names should never be linked to photographic or video material without written permission from the child's parent;
- Wherever possible children should be photographed in groups rather than as individuals;
- No link should be made between an individual and any home address (including simply street names);
- Where the person publishing material suspects that there may be child protection issues at stake then serious consideration must be taken as to whether that material may be published or not. In the case of a simple piece of artwork or writing, this may well be fine, but images of that child should not be published. If in any doubt at all, refer to the person responsible for child protection.
- All parents are required to sign a document on entry indicating their consent to their child's image being taken.

As a school we will ensure that if we publish any photographs or videos of children online, we:

- Will try to ensure that their parents or guardians have given us written permission
- Will ensure if we do not have permission to use the image of a particular child, we will make them unrecognisable to ensure that they are not left out of situations unnecessarily
- Will not include a child's image and their name together without permission from the parents or guardians e.g. if the child has won an award; to appear in a newspaper; or on television.
- Will ensure that children are in appropriate dress and we do not include images of children who are taking part in swimming activities

- Ask that if a parent, guardian or child wishes, they can request that a photograph is removed. This request can be made verbally or in writing to the child's teacher or to the E-Learning Leader. We will endeavour to remove the photograph as soon as possible
- Will provide new parents with a photo permission letter upon their arrival into school
- Will ask parents or guardians to not record video or take digital images at public events e.g. school play or sports day.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication

Consent of Adults Who Work at the School

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

E-Safety

Linked to 360Safe E-Safety Guidelines and Hertfordshire Guidance

At Holy Trinity Rosehill we take E-safety very seriously. We will ensure that it is taught often throughout the children's Computing and PSHE sessions as necessary. We will also provide children with dedicated e-safety lessons where appropriate. Children will be taught how to act online and how to minimise the risk when working on the internet. Pupils will also be taught about managing passwords, respecting copyright and other elements of this policy that are relevant to them.

All children will be taught about the Acceptable Use Policy and will sign a copy related to their age phase. These will be stored by the Admin Team. All staff will also complete an AUP.

If a teacher suspects an E-safety issue within school they should make notes related to the incident in accordance to anti-bullying and behaviour policies. This should then be reported to the E-Learning Leader and head teacher and recorded as appropriate.
If children receive an email that they believe to be inappropriate then they should forward it on to their teacher and/or the E-Learning Leader who will investigate.

Monitoring

The E-Learning Leader, Shadow E-Learning Coordinator or member of the SLMT may inspect any ICT equipment owned or leased by the school at any time without prior notice.

The E-Learning Leader, Shadow E-Learning Coordinator or member of the SLMT may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

The E-Learning Leader, Shadow E-Learning Coordinator or member of the SLMT may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by The E-Learning Leader, Shadow E-Learning Coordinator or member of the SLMT will comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using school equipment may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school hardware, software or services from the offending individual.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

Incident

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows: The E-Learning Leader, Shadow E-Learning Coordinator or member of the SLMT.

All e-safety incidents should be logged on the school's CPOMS service.

Complaints

Incidents regarding the misuse of the Internet by students will be delegated to the E-Learning Leader who will decide which additional evidence should be gathered or recorded. A partnership approach with parents will be encouraged. Any complaint about staff misuse will be referred to the head teacher. Complaints of a child protection nature must be dealt with in accordance with child protection procedures.

Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinator or Headteacher. Incidents should be logged and the **Flowcharts for Managing an eSafety Incident** should be followed.

Inappropriate Material

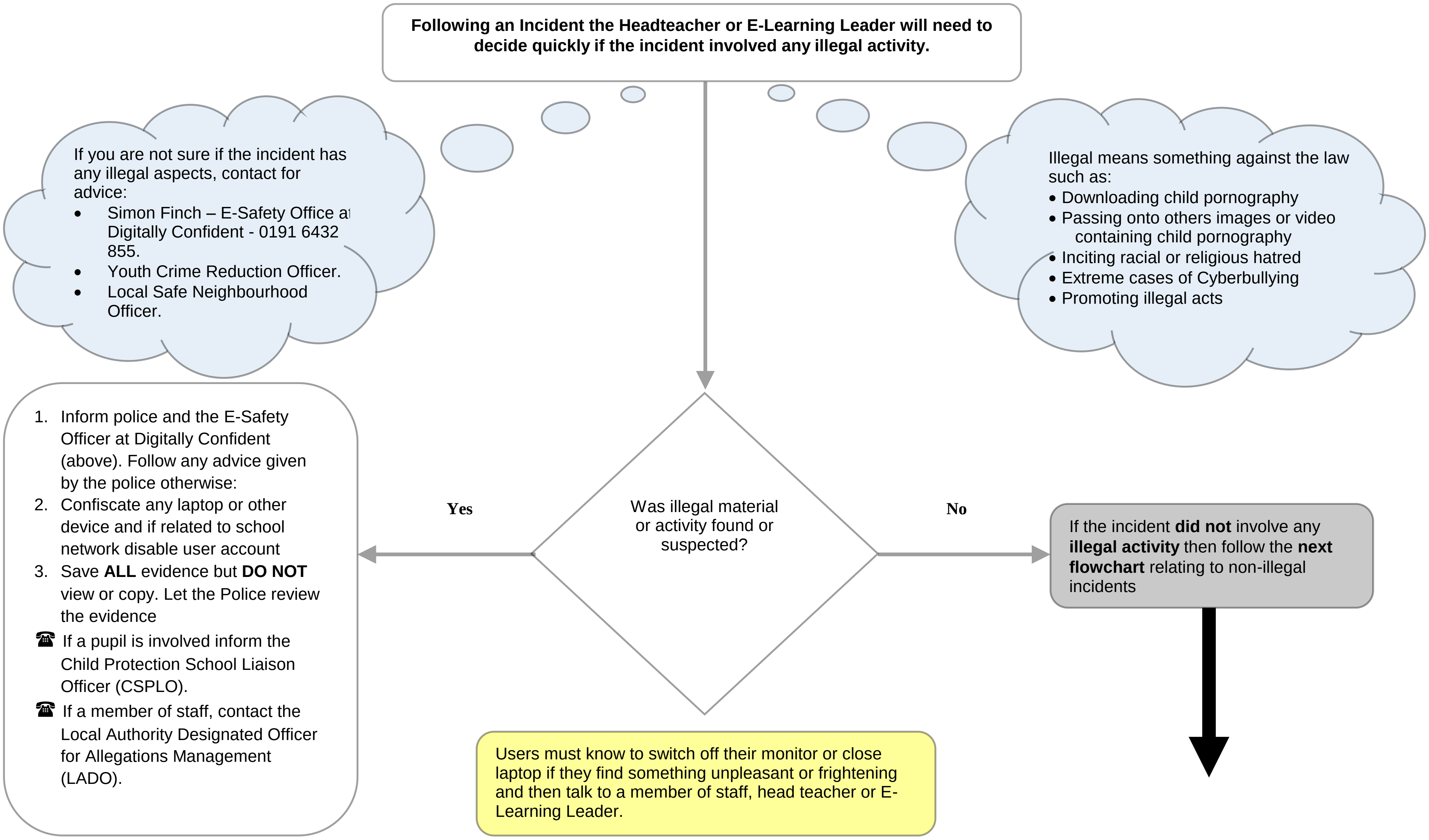
- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the E-Learning Coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Headteacher and E-Learning Leader Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)
- Users are made aware of sanctions relating to the misuse or misconduct through the acceptable use policy.

Flowcharts for Managing an eSafety Incident

These three flowcharts have been developed by the HSCB eSafety subgroup and are designed to help schools successfully manage eSafety incidents. They are based upon guidance from the Herts for Learning Team.

Flowchart to support decisions related to an illegal eSafety Incident

For Head Teachers, Senior Leaders and E-Learning Leaders/Coordinators



Following an Incident the Headteacher or E-Learning Leader will need to decide quickly if the incident involved any illegal activity.

If you are not sure if the incident has any illegal aspects, contact for advice:

- Simon Finch – E-Safety Office at Digitally Confident - 0191 6432 855.
- Youth Crime Reduction Officer.
- Local Safe Neighbourhood Officer.

Illegal means something against the law such as:

- Downloading child pornography
- Passing onto others images or video containing child pornography
- Inciting racial or religious hatred
- Extreme cases of Cyberbullying
- Promoting illegal acts

Was illegal material or activity found or suspected?

Yes

1. Inform police and the E-Safety Officer at Digitally Confident (above). Follow any advice given by the police otherwise:
2. Confiscate any laptop or other device and if related to school network disable user account
3. Save **ALL** evidence but **DO NOT** view or copy. Let the Police review the evidence

☎ If a pupil is involved inform the Child Protection School Liaison Officer (CSPLO).

☎ If a member of staff, contact the Local Authority Designated Officer for Allegations Management (LADO).

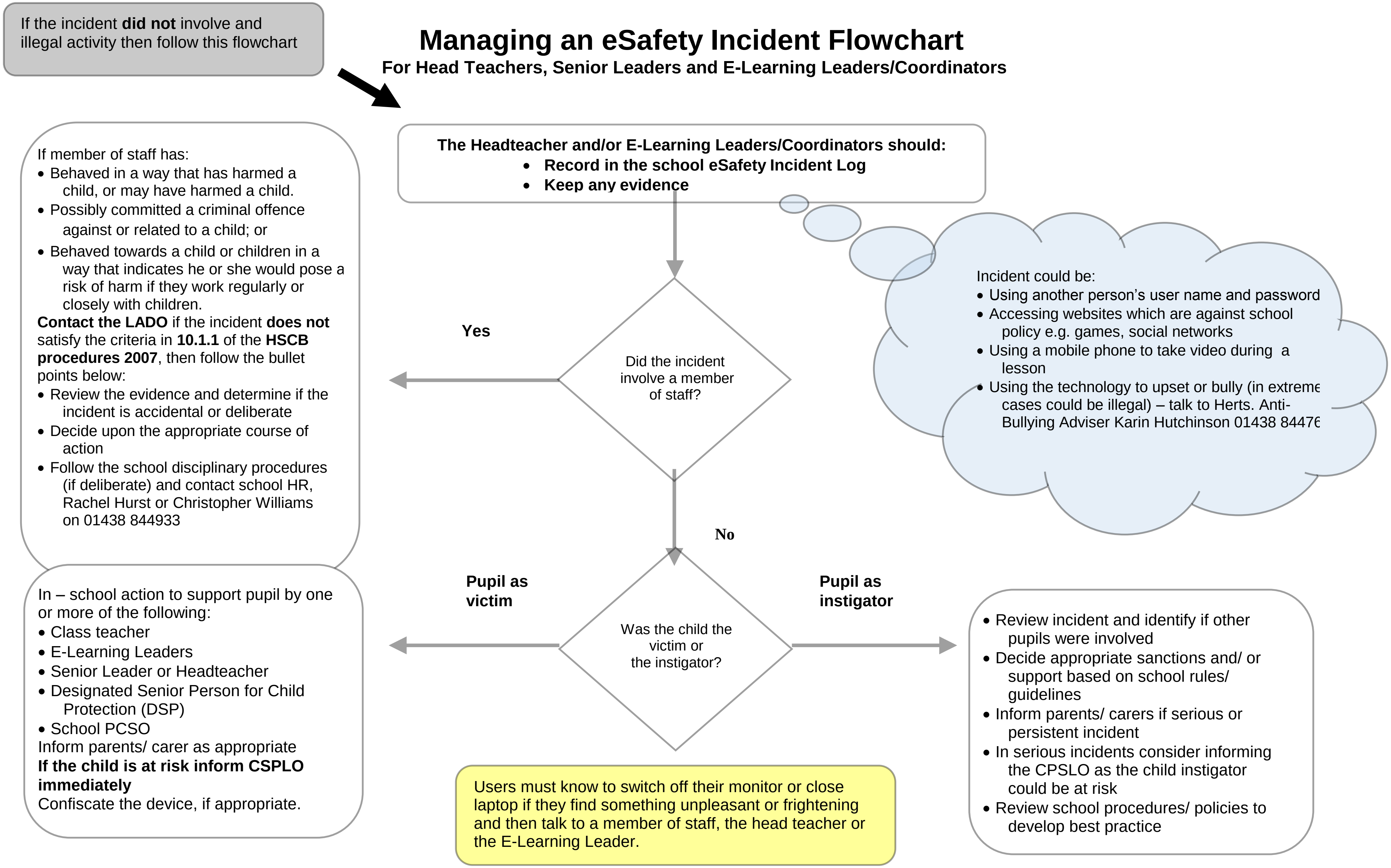
No

If the incident **did not** involve any **illegal activity** then follow the **next flowchart** relating to non-illegal incidents

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff, head teacher or E-Learning Leader.

Managing an eSafety Incident Flowchart

For Head Teachers, Senior Leaders and E-Learning Leaders/Coordinators



If the incident **did not** involve and illegal activity then follow this flowchart

The Headteacher and/or E-Learning Leaders/Coordinators should:

- **Record in the school eSafety Incident Log**
- **Keep any evidence**

Did the incident involve a member of staff?

Yes

If member of staff has:

- Behaved in a way that has harmed a child, or may have harmed a child.
- Possibly committed a criminal offence against or related to a child; or
- Behaved towards a child or children in a way that indicates he or she would pose a risk of harm if they work regularly or closely with children.

Contact the LADO if the incident **does not** satisfy the criteria in **10.1.1** of the **HSCB procedures 2007**, then follow the bullet points below:

- Review the evidence and determine if the incident is accidental or deliberate
- Decide upon the appropriate course of action
- Follow the school disciplinary procedures (if deliberate) and contact school HR, Rachel Hurst or Christopher Williams on 01438 844933

Incident could be:

- Using another person's user name and password
- Accessing websites which are against school policy e.g. games, social networks
- Using a mobile phone to take video during a lesson
- Using the technology to upset or bully (in extreme cases could be illegal) – talk to Herts. Anti-Bullying Adviser Karin Hutchinson 01438 84476

No

Was the child the victim or the instigator?

Pupil as victim

In – school action to support pupil by one or more of the following:

- Class teacher
- E-Learning Leaders
- Senior Leader or Headteacher
- Designated Senior Person for Child Protection (DSP)
- School PCSO

Inform parents/ carer as appropriate

If the child is at risk inform CSPLO immediately

Confiscate the device, if appropriate.

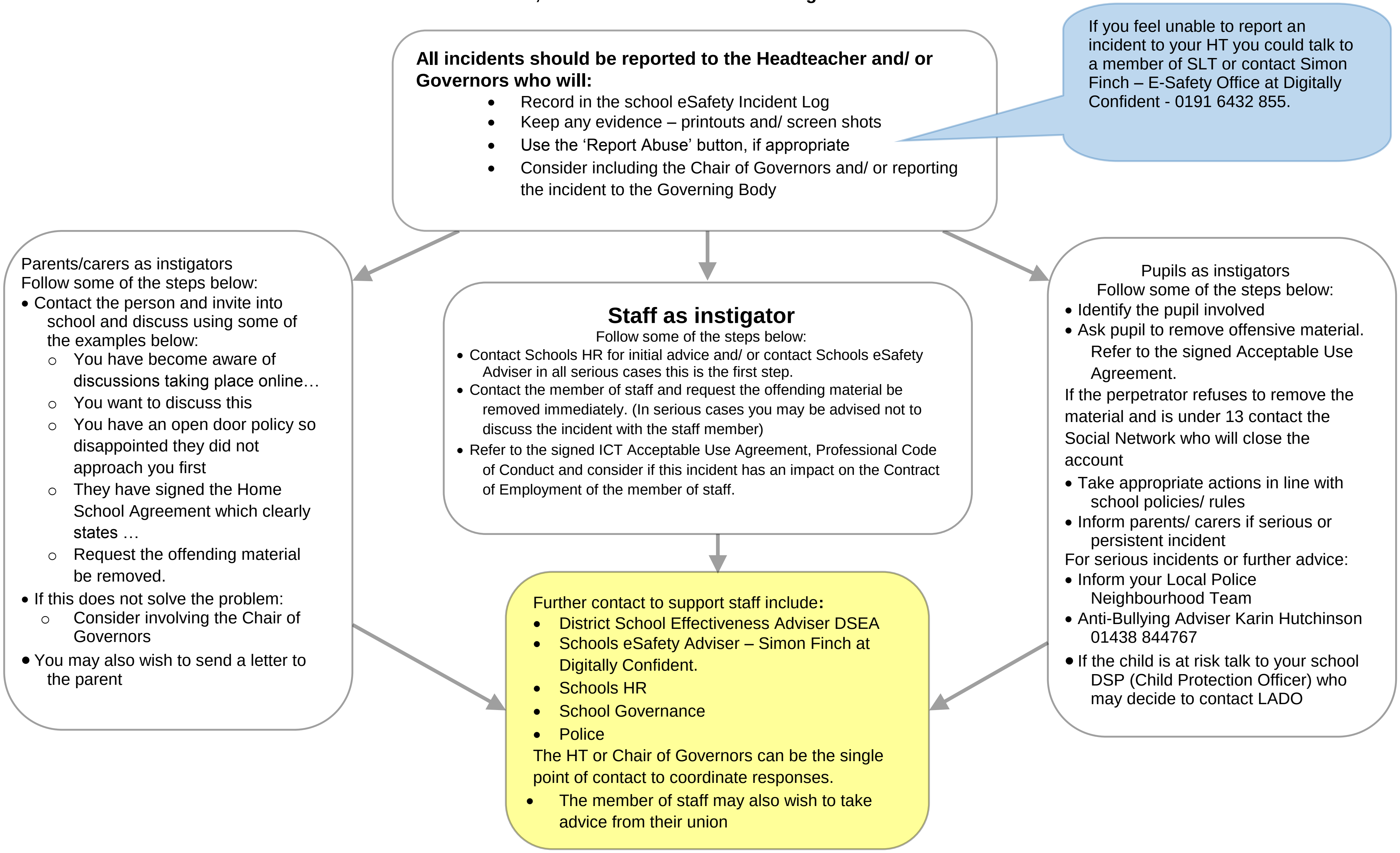
Pupil as instigator

- Review incident and identify if other pupils were involved
- Decide appropriate sanctions and/ or support based on school rules/ guidelines
- Inform parents/ carers if serious or persistent incident
- In serious incidents consider informing the CPSLO as the child instigator could be at risk
- Review school procedures/ policies to develop best practice

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff, the head teacher or the E-Learning Leader.

Managing an eSafety Incident Flowchart involving staff as victims

For Head Teachers, Senior Leaders and E-Learning Leaders/Coordinators



All incidents should be reported to the Headteacher and/ or Governors who will:

- Record in the school eSafety Incident Log
- Keep any evidence – printouts and/ screen shots
- Use the 'Report Abuse' button, if appropriate
- Consider including the Chair of Governors and/ or reporting the incident to the Governing Body

If you feel unable to report an incident to your HT you could talk to a member of SLT or contact Simon Finch – E-Safety Office at Digitally Confident - 0191 6432 855.

Parents/carers as instigators
Follow some of the steps below:

- Contact the person and invite into school and discuss using some of the examples below:
  - You have become aware of discussions taking place online…
  - You want to discuss this
  - You have an open door policy so disappointed they did not approach you first
  - They have signed the Home School Agreement which clearly states …
  - Request the offending material be removed.
- If this does not solve the problem:
  - Consider involving the Chair of Governors
- You may also wish to send a letter to the parent

Staff as instigator

Follow some of the steps below:

- Contact Schools HR for initial advice and/ or contact Schools eSafety Adviser in all serious cases this is the first step.
- Contact the member of staff and request the offending material be removed immediately. (In serious cases you may be advised not to discuss the incident with the staff member)
- Refer to the signed ICT Acceptable Use Agreement, Professional Code of Conduct and consider if this incident has an impact on the Contract of Employment of the member of staff.

Pupils as instigators
Follow some of the steps below:

- Identify the pupil involved
- Ask pupil to remove offensive material. Refer to the signed Acceptable Use Agreement.

If the perpetrator refuses to remove the material and is under 13 contact the Social Network who will close the account

- Take appropriate actions in line with school policies/ rules
- Inform parents/ carers if serious or persistent incident

For serious incidents or further advice:

- Inform your Local Police Neighbourhood Team
- Anti-Bullying Adviser Karin Hutchinson 01438 844767
- If the child is at risk talk to your school DSP (Child Protection Officer) who may decide to contact LADO

Further contact to support staff include**:**

- District School Effectiveness Adviser DSEA
- Schools eSafety Adviser – Simon Finch at Digitally Confident.
- Schools HR
- School Governance
- Police

The HT or Chair of Governors can be the single point of contact to coordinate responses.

- The member of staff may also wish to take advice from their union

Acceptable Use

Copyright and Intellectual Property Right (IPR)
Copyright of materials should be respected. This includes when downloading material and/or copying from printed materials. Staff should not remove logos or trademarks unless the terms of the website allow it.

Staff should check permission rights before using materials, particularly images, from the internet. Children will be taught in Key Stage 2 to begin to consider the use of images from the internet. In year 3/4 they will have discussions about the proper use of images with questions such as 'Is it OK to use an image we find online?' As they progress to year 5/6 some children should start referencing the sites they have used. This could be as simple as putting the name of the site the image came from or a hyperlink. It is not expected for children to include a full reference but to be *aware* that it is not acceptable to take images directly from the internet without some thought on their use.

All materials created by staff whilst in employment of the school belong to the school and should not be used for financial gain. This is in accordance with guidelines laid out by the local authority.

Email
The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and how to behave responsible online.

Managing Email

- The school gives all staff & governors their own e-mail account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

- Staff & governors should use their school email for all professional communication.

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- E-mails created or received as part of your school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
  - Delete or archive all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- The forwarding of chain emails is not permitted in school. However the school has set up a dummy account (**reporting@htrschool.net**) to allow pupils to forward any chain emails causing them anxiety.
- All pupil e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail
- Staff must inform (the Headteacher, E-Learning Leader or Shadow E-Learning Coordinator) if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the Computing Programme of Study
- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Sending e-mails

- Use your own school e-mail account so that you are clearly identified as the originator of a message

- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments

- School e-mail is not to be used for personal advertising or business

Receiving e-mails

- Check your e-mail regularly

- Activate your 'out-of-office' notification when away for extended periods

- Never open attachments from an untrusted source; consult your network manager first

E-mailing Personal, Sensitive, Confidential or Classified Information

- Where your conclusion is that e-mail must be used to transmit such data:

  Either:
  Obtain express consent from your manager to provide the information by e-mail and exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

  - Encrypt and password protect. See http://www.thegrid.org.uk/info/dataprotection/#securedata

  - Send from the secure @sbcschools.org.uk domain

  - Verify the details, including accurate e-mail address, of any intended recipient of the information

  - Verify (by phoning) the details of a requestor before responding to e-mail requests for information

  - Do not copy or forward the e-mail to any more recipients than is absolutely necessary

- Do not send the information to any person whose details you have been unable to separately verify (usually by phone)

- Send the information as an encrypted document **attached** to an e-mail

- Provide the encryption key or password by a **separate** contact with the recipient(s)

- Do not identify such information in the subject line of any e-mail

- Request confirmation of safe receipt

Data Storage

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

Staff should be aware that they should not transfer personal data such as reports, IEPs and contact information on to personal devices unless strictly necessary. This data should then be removed as soon as possible. When using a personal laptop or device containing student data, staff should be extra vigilant to not leave this device lying around or on display e.g. in a parked car. Staff should adhere to the following rules:

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your manager
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

Staff are forbidden to use their own removable personal storage devices (e.g. USB drives) on the school network system. The only removable storage devices that can be used on the network are school-provided encrypted memory drives.

Work should always be saved to the school system rather than removable media as the school system is backed up regularly and is secure. Removable devices should only be used in the short term and never as a permanent storage solution.

Mobile Phones and Handheld Devices

(Linked to 360Safe Mobile Phone Guidelines)
Staff may attempt to connect their phone to the school's guest wireless network in accordance with the network guidelines in the Acceptable Use Policy but should be aware that this may not work due to the settings available on their phones.

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

Responding to unacceptable use by staff

Failure to comply with the guidelines and expectations set out for them could lead to sanctions being imposed on staff and possible disciplinary action being taken in accordance with the school's policy and possibly the law.

Responding to unacceptable use by pupils

Pupils should be aware that all e-safety issues will be dealt with quickly and effectively. When dealing with unacceptable use, staff should follow the behaviour policy and if necessary, the anti-bullying policy. Children may have restrictions placed on their account for a short time.

Coordination and Management

- The school has an ICT technician, Michael Thain, from ONE ITSS, who works in school on a Thursday afternoon.
- Mr M. Waller is the E-Learning coordinator and works as part of the school's Senior Leadership and Management Team and Mrs C. Pearson is the Shadow E-Learning Coordinator. Together they are responsible for:
  - producing an E-Learning development plan and for the implementation of the E-Learning policy across the school.
  - Progress of the plan will be monitored as stated in the plan and reported on termly in the Head teacher's report to Governors.
- A governor will be invited to take a particular interest in Computing in the school.

The Headteacher & SMT (including the E-Learning Leader) are responsible for:

- ensuring there is a shared vision for ICT within the school
- ensuring consistent implementation of ICT Policy & Internet Policy
- ensuring staff access to ICT and identifying ICT support needed by individual staff

The E-Learning Leader and Shadow E-Learning Coordinator are responsible for:

- the day-to-day implementation of the E-Learning Policy and aspects of the E-learning development plan as well as the implementation of an Computing scheme of work
- reviewing the E-Learning policy
- Computing monitoring which includes classroom observations, scrutiny of work and planning and discussions with pupils
- co-ordinating the integration of ICT into the curriculum ensuring continuity and progression
- co-ordinating e-learning training for staff to raise awareness, build on experience and develop confidence
- working with subject co-ordinators and staff to encourage the use of ICT as a teaching & learning tool across the curriculum
- overseeing equipment maintenance and liaising with our IT technician
- co-ordinating the purchase and allocation of digital resources depending on budget priorities
- managing and updating the htrschool.net system which includes the school websites and class blogs
- managing additional services relating to the computing and ICT across the curriculum such as Education City, Espresso Primary and Purplemash.

Teachers are responsible for:

- curriculum development
- planning and teaching Computing and to use ICT within their class. This will be in accordance to the schemes of work provided by the E-Learning Leader/Shadow E-Learning Coordinator (currently the 'Switched On' schemes of work)
- meeting the statutory requirements
- the assessment of pupils
- keeping an electronic portfolio of children's work
- delivering E-Safety units using the schools progression document
- implementing the health and safety policy and practice
- all subject co-ordinators are responsible for integrating effective use of ICT into the scheme of work for their subject.
- reporting IT issues and faults to ONE ITSS through their online helpdesk.
- respond to, and report, and e-safety or cyber bullying issues that they encounter within or out of school in accordance to e-safety procedures as outlined in this policy

All teaching, support and office staff, as a minimum standard of professional competence, are responsible for:

- being capable of using the hardware and software provided to ensure that they can complete their role effectively
- being able to save work (onto a disk, memory stick or the hard drive) and retrieve it
- being able to print work
- being able to use the internet and find information
- being able to send and receive e-mails and access the htrschool.net online system
- being able to use a digital camera and transfer files to a computer

Governors and visitors are responsible for:

- abiding by the guidelines set out for staff and ensure that computers and equipment within school is used safely

The school is responsible for:

- ensuring that parents and pupils are fully aware of ways in which the internet and technologies can be used productively and safely
- ensure that we provide children with the opportunities to excel and achieve when using technologies and will ensure our curriculum is challenging and relevant
- before launching any system or initiative, we will make sure that the children's safety is at the forefront of our thoughts and we will keep parents information as necessary

Pupils are responsible for:

- following the guidelines set out in the AUP
- ensuring that the computers and equipment are used appropriately at all times
- follow the school's behaviour policy when working online
- adhere to the school's anti-bullying policy

Parents are responsible for:

- staying vigilant to the websites and content that their children are accessing out of school.

Entitlement and Equal Opportunities

Entitlement for pupils

- All pupils will be given equal opportunities to access their entitlement of the ICT National Curriculum;
- ICT will be used to help to meet Special Educational Needs of all pupils in order to maximise their access to the curriculum and to support their learning.

Entitlement for staff

The school is committed to providing CPD for all school staff in the field of e-learning. The E-Learning Leader and Shadow E-Learning Coordinator will assess and address staff training needs as part of the annual development plan process or in response to individual needs and requests throughout the year

- Individual teachers should attempt to continually develop their own skills and knowledge, identify their own needs and notify the Shadow E-Learning Leader or E-Learning Coordinator
- Teachers will be encouraged to use technology to produce plans, reports, communications and class labelling

Equal Opportunities and Inclusion

We will ensure that all pupils are provided with opportunities to access the computing curriculum and digital technologies throughout the school. Where necessary, we will endeavour to make adaptations to the environment or provide software that will enable all learners to achieve.

Current Legislation

Acts Relating to Monitoring of Staff email

Data Protection Act 1998
The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000
Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated

with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000
https://ico.org.uk/for-organisations/guide-to-freedom-of-information/