Singleton Church of England Primary School

"Passion for Learning and Passion for Life"

Online Safety Policy

School lead for this policy:	**Amanda Clayton/ Lisa Rund**
Committee with oversight for this policy	**Governance Committee**
Policy to be approved by the **Governance** Committee.	**Summer 2018**
Policy last reviewed by the **Governance** Committee.	**Summer 2017**
Policy due for next review.	**Summer 2019**
Ratified at the Governance Meeting on 8th June 2018. **Chair: Keith Walker**	

School Vision

"To ensure Singleton School, inspired by Christian values, is at the heart of our community, with an outstanding reputation for maturing growth and excellence within our children."

Mission Statement

To be a Christ centred community, where the uniqueness of each individual is recognised and celebrated. We ensure pupils and staff feel loved and valued and that their full potential is realised within a secure, stimulating and happy environment.

Our Core Christian Values

Wisdom
Love
Caring
Endurance
Friendship
Trust

These core values are threaded into all aspects of our school life. Using these as a basis, the following constitute the aims of the school.

School Aims

- As a Christian school there is a family environment in our school with high expectations of behaviour within a framework of love, reconciliation and forgiveness. We recognise that all children are at different stages in their faith journey, as such requiring support appropriate to their individual needs.
- Within our school, a shared and understood code of conduct ensures a consistent message of respect and self-control for adults and children. We encourage good behaviour by showing courtesy, good manners, consideration for the needs of others and respect for the ethos of the school.
- We recognise that high self-esteem, confidence, supportive friends and clear lines of communication with adults help children to behave well. Recognising that parents are also prime educators, we encourage a close partnership between home and school.
- Our school is a place where learning and personal development take place in a climate of trust and confidence, such that children feel secure. We encourage a love of learning, ability to question and think rationally, to show initiative and apply themselves to all tasks conscientiously. They are encouraged to talk and are listened to.
- We deliver a broad and balanced curriculum and, with opportunities for PSHE, equip children with knowledge, skills and vocabulary that they need to develop self-control and respect for others. In doing this, we promote a respect and understanding for the cultural and religious principles of others, particularly those within our own community.
- All staff and volunteers working in school acknowledge their responsibility to act as role models of acceptable behaviour.
- A climate of trust, openness and communication exists between home, school and the wider community. To enable this we work in partnership with the local community and industry to deepen our understanding of the wider world.
- We enable each child to progress towards the realisation of his/her full potential, regardless of age, cultural background, disability, gender, race or religious beliefs. Our performance is continually monitored to raise standards even higher.
- We apply sanctions that are appropriate and consistent, with a clear progression of severity.
- We monitor inappropriate behaviour, as this may indicate emotional and behavioural special needs where a child requires special support to be included in school life. Our Learning Mentor plays a significant role within this area.

CONTENTS

Scope of the policy

This policy has been developed in consultation with staff, pupils, students, parents and the wider community. It applies to all members of the **Singleton C of E School** community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of **Singleton C of E School.**

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / 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 Internet 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.

Singleton C of E School 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 use.

The Acceptable Use of ICT Agreements should be issued to the appropriate users for their signature. These should be retained by a designated member of staff.

Schools should ensure that all persons, including Staff, Governors, Parents, students and pupils, who join the establishment mid-year are made aware of the policy and sign the relevant agreement/s.

The Home/School Agreement should alert parents as to what is acceptable in terms of ICT communications on matters related to the school, its staff and other parents/carers.

After alterations are made and before the ratification stage, the spacing and page numbering of this document should be checked for continuity

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. 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 Internet Safety is therefore an essential part of the school's Internet Safety provision. Children and young people need the help and support of the school to recognise and avoid Internet Safety risks and build their resilience.

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

Currently the internet technologies children and young people are using both inside and outside of the classroom include:

Websites
Apps
E-mail, Instant Messaging and chat rooms
Social Media, including Facebook and Twitter
Mobile/ Smart phones with text, video and/ or web functionality
Other mobile devices including tablets and gaming devices
Online Games
Learning Platforms and Virtual Learning Environments
Blogs and Wikis
Podcasting
Video sharing
Downloading
On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At **Singleton C of E School***,* we understand the responsibility to educate our pupils on Online Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.
Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Monitoring

All internet activity is logged by the school's internet provider. These logs may be monitored by that provider (BT Lancashire One connect) without prior notice. Authorised ICT (Subject leader) staff and governors (Safeguarding subcommittee) may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask the head teacher or senior teacher. Any authorised staff member will be happy to comply with this request.

ICT authorised staff / governors conduct in house monitoring of internet activity on a regular basis. They may also monitor, intercept, access, inspect, record and disclose telephone calls, emails, 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.

ICT authorised staff may, without prior notice, access the email or voicemail 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 ICT authorised staff and 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 ICT 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 ICT 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

For pupils, reference will be made to the school’s behaviour policy.

Incident Reporting

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 Secure ID 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:

Amanda Clayton – DSL / Head teacher

Karen Haigh – DSL / Senior teacher

Matthew Lee – Governor – member of the safeguarding sub-committee (SHE)

Pupil Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Singleton CE Primary School

Pupil Acceptable Use Agreement (Foundation / KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child): ....

Signed (parent): ....

Singleton CE Primary School

Pupil Acceptable Use Agreement (KS2)

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that **Singleton C of E School** will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.
- I will not arrange to meet anyone offline without first seeking permission from an adult. If I do arrange to meet it will only ever be with an adult present.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that **Singleton C of E School's** systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the **Singleton C of E School**'s systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that **Singleton C of E School** also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Signed (child): ....

Signed (parent): ....

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor / Student Teachers
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Alex Davies the Chair of Governors (Safeguarding Governor.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure email system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of Lisa Rund and Matthew Lee (ICT subject lead / ICT support Governor)
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online Internet Safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's Internet Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I will not use personal electronic devices (including smart watches) in public areas of the school between the hours of 8:30am and 5:30pm, except in the staff room and where there are signs to indicate this.
- I understand this forms part of the terms and conditions set out in my contract of employment

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ………..………………………… Date ……………………

Full Name ……………………………………….. (printed)

Job title ……………………………………………………………….

Staff Professional Responsibilities

The HSCB Internet Safety subgroup group have produced a clear summary of **professional responsibilities related to the use of ICT** which has been endorsed by unions. To download visit http://www.thegrid.org.uk/eservices/safety/policies.shtml

Professional responsiblities – Summary of Advice from the following unionswhaen using any form of ICT including the internet in your school.

- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.
- Do not talk about your professional role in any capacity when using social media such as Facebook and You Tube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school e-mail address, school mobile phone and school video camera.
- Do not give out your personal details, such as a mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others
- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately
- Only take images of pupils and/ staff for professional purposes, in accordance with school policy and with the knowledge of SLT
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ensure that your activity on line, both in school and outside school, will not being your organisation or professional role into disrepute.

You have a duty to report any Internet Safety incident which may impact on you, your professionalism or your organisation

Computer Viruses

- All files downloaded from the Internet, received via email or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.

- Never interfere with any anti-virus software installed on school ICT equipment.

- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through Lisa Rund.

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Data Security

Data Protection: key responsibilities for School Heads and Governors

The accessing and appropriate use of school data is taken very seriously. HCC guidance documents can be found at:

http://www.thegrid.org.uk/info/dataprotection/index.shtml#data

Security

- The school gives relevant staff access to its Management Information System, with a unique username and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff keeps all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal or sensitive information contained in documents faxed, copied, scanned or printed. This is particularly important when using shared copiers (multi-function print, fax, scan and copiers) are used
- Anyone sending a confidential or sensitive fax should notify the recipient before it is sent

Protective Marking of Official Information

Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them, in line with local business processes.

- There is no requirement to mark routine OFFICIAL information.
- Optional descriptors can be used to distinguish specific type of information.
- Use of descriptors is at an organisation's discretion.
- Existing information does not need to be remarked.

In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: '**OFFICIAL–SENSITIVE**'

Relevant Responsible Persons

Senior members of staff/ governors should be familiar with information risks and the school's response. The SHE Committee – which forms part of the governing body, has the following responsibilities:

- They lead on the information risk policy and risk assessment
- They advise school staff on appropriate use of school technology
- They act as an advocate for information risk management
- They monitor the implementation of the Internet Safety Policy

The named Governor is **MATTHEW LEE**

The Office of Public Sector Information has produced *Managing Information Risk*, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support relevant responsible staff members in their role.

Disposal of Redundant ICT Equipment Policy

All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen
Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Data Protection Act 1998
https://ico.org.uk/for-organisations/education/
Electricity at Work Regulations 1989
http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal
The school's disposal record will include:

- Date item disposed of
- Authorisation for disposal, including:
- Verification of software licensing
- Any personal data likely to be held on the storage media? *
- How it was disposed of e.g. waste, gift, sale
- Name of person & / or organisation who received the disposed item
- If personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.
- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

Introduction

http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

The Waste Electrical and Electronic Equipment Regulations 2006

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

Information Commissioner website
https://ico.org.uk/

Data Protection Act – data protection guide, including the 8 principles
https://ico.org.uk/for-organisations/education/

PC Disposal – SITSS Information
http://www.thegrid.org.uk/info/traded/sitss/services/computer_management/pc_disposal

Email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email 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 email in relation to their age and how to behave responsibly online.

Staff should use a school email account for all official communication to ensure that children are protected through the traceability of all emails through the school email system. In addition. This is to help mitigate the chance of issues occurring and is an essential element of the safeguarding agenda.

Managing email

- The school gives all staff their own email 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 emails and avoids the risk of personal profile information being revealed.

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

- It is the responsibility of each account holder to keep the password secure. For the Internet Safety and security of users and recipients, all mail is filtered and logged; if necessary email 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 email addresses.

- The school has a standard disclaimer which should be included on all email correspondence, stating that, the information is intended for the addressee only and that the school has taken reasonable steps to ensure that outgoing communications do not contain malicious software but it is the receivers responsibility to carry out any checks on the email before accepting the email and opening any attachments.
  - The responsibility for adding this disclaimer lies with the account holder.

- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

- Staff sending emails to external organisations, parents or pupils are advised to cc. the Head teacher, line manager or designated line manager.

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

- Emails created or received as part of your school job 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 email account as follows:
  - Delete all emails of short-term value.
  - Organise email into folders and carry out frequent house-keeping on all folders and archives.
- All pupil email 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 email 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 email.

- Staff must inform (the Internet Safety coordinator or line manager) if they receive an offensive email.

- Pupils are introduced to email as part of the Computing Programme of Study.

- However, you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply.

Sending emails

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section Emailing Personal or Confidential Information.

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

- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate

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

- School email is not to be used for personal advertising

Receiving emails

- Check your email regularly
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source; consult your network manager first
- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

Emailing Personal or Confidential Information

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

  Either:
  Use Lancashire's web-based Secure File Exchange portal that enables schools to send and receive confidential files securely
  http://www.thegrid.org.uk/eservices/schoolsfx.shtml

  Or:
  Obtain express consent from your manager to provide the information by email and exercise caution when sending the email and always follow these checks before releasing the email:

  - Encrypt and password protect. See http://www.thegrid.org.uk/info/dataprotection/#securedata
  - Verify the details, including accurate email address, of any intended recipient of the information
  - Verify (by phoning) the details of a requestor before responding to email requests for information
  - Do not copy or forward the email 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 email
  - 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 email
  - Request confirmation of safe receipt

Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the schools' Internet Safety rules.

However, staff is aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Internet Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Internet Safety. Internet activities are planned and well managed for these children and young people.

Online Safety

Online Safety - Roles and Responsibilities

As Online Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Internet Safety co-ordinator in this school is ***Lisa Rund*** who has been designated this role and will be supported by **Matthew Lee** (Governor) and **Karen Haigh** (DSL). All members of the school community have been made aware of who holds this post. It is the role of the Internet Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Lancashire county Council, CEOP (Child Exploitation and Online Protection) and Child net.

Senior Management and governors are updated by the Head/ Internet Safety co-ordinator / Internet Safety Governor and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHCE.

Internet Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for Internet Safety guidance to be given to the pupils on a regular and meaningful basis. Internet Safety is embedded within our curriculum and we continually look for new opportunities to promote Internet Safety.

- The school has a framework for teaching internet skills in Computing/ICT/ PSCHE lessons this can be found on the school website – LONG TERM PLANNERS. **Karen Haigh** regularly reviews and updates these to ensure that PREVENT materials and safeguarding recommendations are clear and up to date
- The school provides opportunities within a range of curriculum areas to teach about Internet Safety
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the Internet Safety curriculum
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities
- Pupils are aware of the impact of Cyberbullying and know how to seek help if

they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Child line or the 'CEOP report abuse' button

Internet Safety Skills Development for Staff

Possible statements

- Our staff receive regular information and training on Internet Safety and how they can promote the 'Stay Safe' online messages in the form of Staff meetings, external people coming in to deliver programmes to the children etc
- Details of the ongoing staff / governor training programme can be found *in the staff meeting minute, in the safeguarding training records, in the record of staff course, SHE meeting minute. The ICT/ Internet Safety subject lead – goes on courses regularly to ensure that we are constantly up to date in terms of Internet Safety.*
- New staff receive information on the school's acceptable use policy as part of their induction – safeguarding pack.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of Internet Safety and know what to do in the event of misuse of technology by any member of the school community (see Internet Safety Coordinator).
- All staff are encouraged to incorporate Internet Safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

Managing the School Internet Safety Messages

- We endeavour to embed Internet Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The Internet Safety policy will be introduced to the pupils at the start of each school year.
- Internet Safety posters will be prominently displayed.
- The key Internet Safety advice will be promoted widely through school displays, newsletters, class activities and so on.

Incident Reporting, Internet Safety Incident Log & Infringements

Incident Reporting

Following an incident the correct protocols should be followed, these are outlined in the flowcharts on pages 27 – 30. **Singleton C of E School** regards online safety as a wider community issue and we will deal rigorously with out of school online safety incidents that relate to members of the school community.

Any incidents 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 or Internet Safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Information Asset Owner. See Page 15.

Singleton C of E School – Internet Safety Incident Log

All Internet Safety incidents should be recorded by the Internet Safety Coordinator and shared each Half term with Matthew Lee – Internet Safety Governor. This incident log will be monitored termly by the 'Governance Committee' through feedback from Matthew Lee Governor. Any incidents involving Cyber bullying may also need to be recorded elsewhere.

Singleton C of E School   Internet Safety Incident Log/ Web monitoring log

All Internet Safety incidents should be recorded by the Internet Safety Coordinator **Lisa Rund** and shared each half term with **Matthew Lee** – Internet Safety Governor. Each half term Matthew Lee and Lisa Rund will randomly monitor web activity. This incident / web activity log will be monitored termly by the 'Governance Committee' through feedback from **Matthew Lee** Governor. Any incidents involving Cyber bullying should be logged but may also need to be recorded elsewhere in more detailed chronologies.

Date & time	Name of pupil or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

Misuse and Infringements

Complaints

Complaints and/ or issues relating to Internet Safety should be made to the Internet Safety co-ordinator or Head teacher.

Incidents should be logged – staff must hand write an account of the incident and include dates and times and sign it.

Referrals should be made to the DSL using the safeguarding referral forms located in the staffroom.

The **Flowcharts for Managing an Internet Safety Incident** should be followed. (See section 3 of the Internet Safety folder).

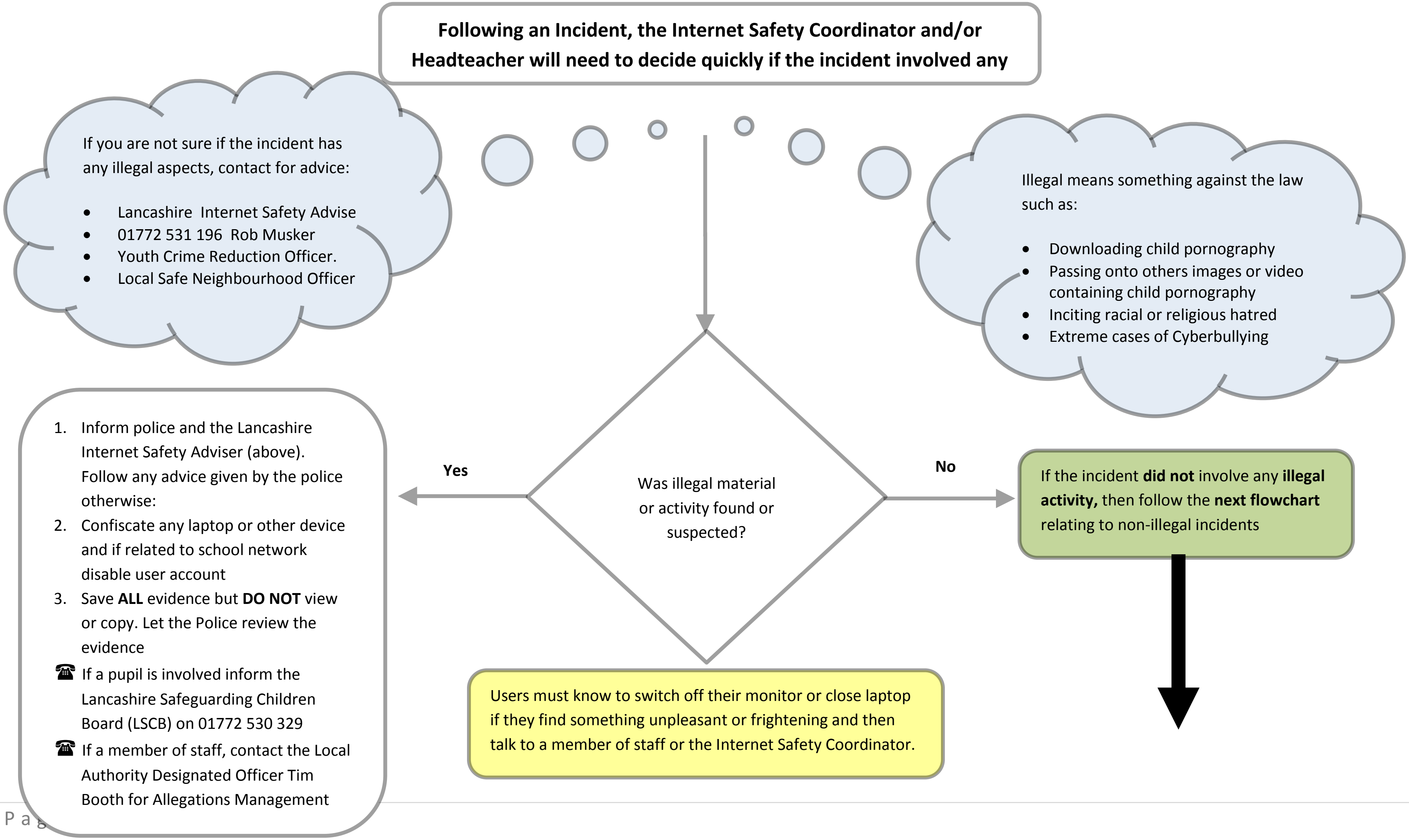
Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Internet Safety co-ordinator.
- 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 Head teacher and potentially the Internet Safety coordinator and safety governor will commence. (The inclusion of the e- safety coordinator and governor will be dependent on the nature of the incident for example if technical skill is required to retrieve information as evidence off the computer.) 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 by the code of conduct policy and the disciplinary policy and behavioural policy.

Flowcharts for Managing an Internet Safety Incident

These three flowcharts have been developed by Singleton School using the support materials developed by the HSCB (Hertfordshire Grid for learning) Internet Safety subgroup and are designed to help schools successfully manage Internet Safety incidents.

Singleton Church of England Primary School Flowchart to support decisions related to an illegal Internet Safety Incident For Headteachers, Senior Leaders and Internet Safety Coordinators.



Following an Incident, the Internet Safety Coordinator and/or Headteacher will need to decide quickly if the incident involved any

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

- Lancashire Internet Safety Advise
- 01772 531 196 Rob Musker
- 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

Was illegal material or activity found or suspected?

Yes

1. Inform police and the Lancashire Internet Safety Adviser (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 Lancashire Safeguarding Children Board (LSCB) on 01772 530 329

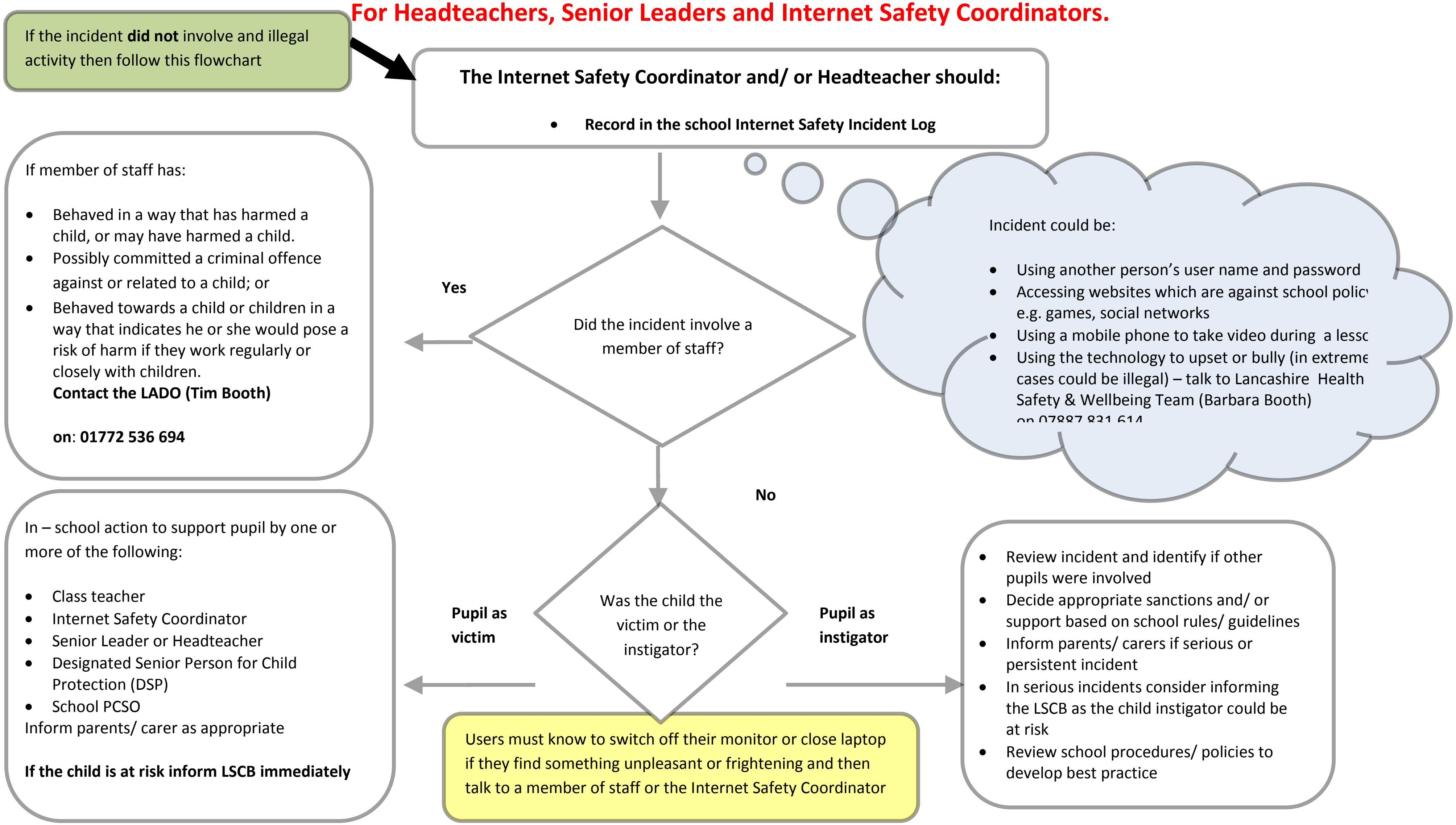
☎ If a member of staff, contact the Local Authority Designated Officer Tim Booth for Allegations Management

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 or the Internet Safety Coordinator.

Singleton Church of England Primary School Managing an Internet Safety Incident Flowchart For Headteachers, Senior Leaders and Internet Safety Coordinators.



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

The Internet Safety Coordinator and/ or Headteacher should:

- **Record in the school Internet Safety Incident Log**

Incident could be:

- Using another person's user name and password
- Accessing websites which are against school polic e.g. games, social networks
- Using a mobile phone to take video during a lesso
- Using the technology to upset or bully (in extreme cases could be illegal) – talk to Lancashire Health Safety & Wellbeing Team (Barbara Booth) on 07887 831 614

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 (Tim Booth)

  on: 01772 536 694

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
- Internet Safety Coordinator
- Senior Leader or Headteacher
- Designated Senior Person for Child Protection (DSP)
- School PCSO

Inform parents/ carer as appropriate

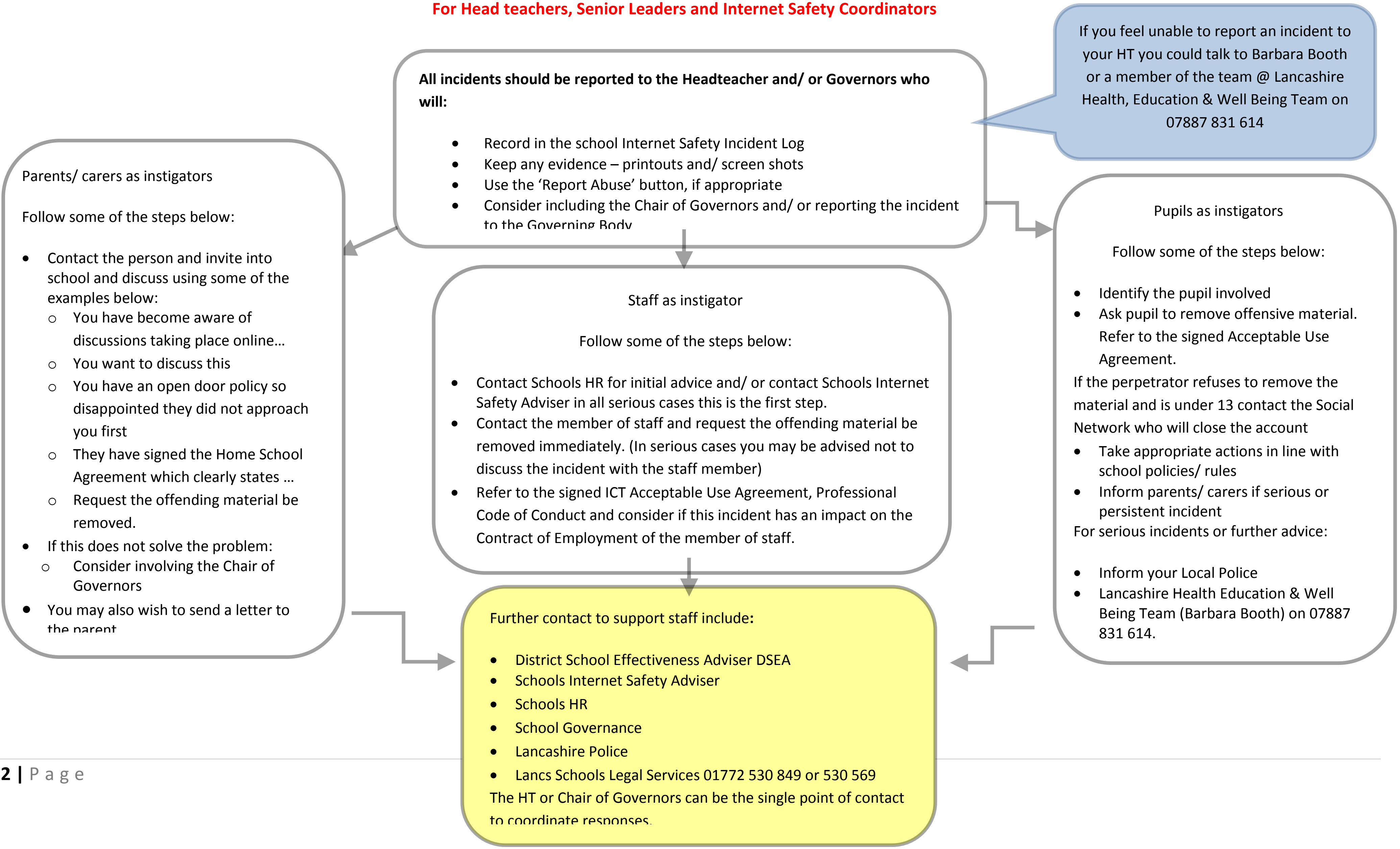
If the child is at risk inform LSCB immediately

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 LSCB 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 or the Internet Safety Coordinator

Singleton Church of England Primary School Managing an Internet Safety Incident Flowchart involving staff as victims
For Head teachers, Senior Leaders and Internet Safety Coordinators



If you feel unable to report an incident to your HT you could talk to Barbara Booth or a member of the team @ Lancashire Health, Education & Well Being Team on 07887 831 614

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

- Record in the school Internet Safety 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

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 Internet Safety 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
- Lancashire Health Education & Well Being Team (Barbara Booth) on 07887 831 614.

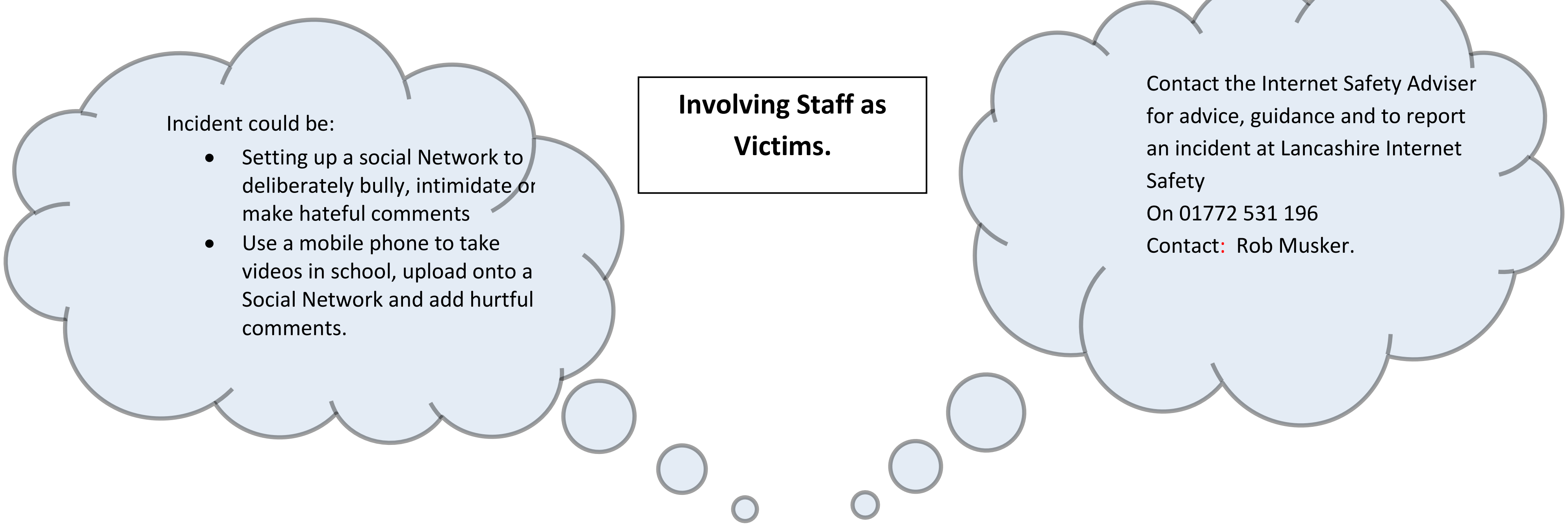
Further contact to support staff include:

- District School Effectiveness Adviser DSEA
- Schools Internet Safety Adviser
- Schools HR
- School Governance
- Lancashire Police
- Lancs Schools Legal Services 01772 530 849 or 530 569

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

Singleton Church of England Primary School Managing an Internet Safety Incident Flowchart involving staff as victims

For Head teachers, Senior Leaders and Internet Safety Coordinators



Incident could be:

- Setting up a social Network to deliberately bully, intimidate or make hateful comments
- Use a mobile phone to take videos in school, upload onto a Social Network and add hurtful comments.

Involving Staff as Victims.

Contact the Internet Safety Adviser for advice, guidance and to report an incident at Lancashire Internet Safety
On 01772 531 196
Contact: Rob Musker.

Staff, parents, children, young people, governors and others can all become involved in an Internet Safety incident either as an investigator or victim. To help reduce the number of incidents we suggest that all schools and governing bodies consider the following:

Ways to prevent Internet Safety incidents

- Have up to-date ICT Acceptable Use Policies for All users with signed user agreements. Some policies can be found on Lancs NGfL website.
- Include a sentence in your Home School Agreement.
  - We will support the school approach to online Internet Safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- Hold regular Internet Safety awareness / update sessions for staff, governors, parents and carers.
- Have an effective school complaints system which all parents, carers and others feel confident will address their concerns.
- Embed Internet Safety throughout the curriculum and beyond.

Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.
All internet use through the Lancashire network (BT Lancashire Services Ltd – One Connect) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Lisa Rund and **Mathew Lee** – will randomly monitor – at least once a half term and records of this will be kept in section D of the e- safety folder.

Mathew Lee will report back to the 'Governance Committee'

Managing the Internet

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity
- Staff will preview any recommended sites, online services, software and apps before use
- Searching for images through open search engines is discouraged when working with pupils
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources
- All users must observe copyright of materials from electronic resources

Internet Use

See acceptable use agreements for clear guidelines

Infrastructure

Schools subscribing to the web filtering service Lancashire network (BT Lancashire Services Ltd – One Connect) have the benefit of monitored web activity.

However, the monitoring is more in the form that they can identify if any inappropriate activity has taken place if asked. All though they have a collection of data they do not inform schools if there has been a serious breech. As a School we have to check ourselves and then could contact BT Lancashire Services Ltd – One Connect – for data information if we had identified a breech

Our school also employs some additional web-filtering which is the responsibility of

Lisa Rund and Matthew Lee

Singleton School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

Lisa Rund and Matthew Lee carry out random monitoring once a half term.

- The school does not allow pupils access to internet logs
- The school uses management control tools for controlling and monitoring workstations – **Lisa Rund is the only named person with administrator rights and codes. The only other person with access codes is Amanda Clayton**
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the Internet Safety coordinator or teacher as appropriate
- It is the responsibility of the school, by delegation to **Lisa Rund and Matthew Lee**, to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from **Lisa Rund**
- If there are any issues related to viruses or anti-virus software, Lisa Rund must be informed

Managing Other Online Technologies

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities.

However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking and online games websites to pupils within school
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Our pupils are asked to report any incidents of Cyberbullying to the school
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Headteacher

When signing up to online services that require the uploading of what could be deemed as **personal or sensitive data**, schools should check terms and conditions regarding the location of storage. Please see the Safe Harbor Agreement Statement http://www.thegrid.org.uk/info/dataprotection/#data
Also: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/10/ico-response-to-ecj-ruling-on-personal-data-to-us-safe-harbor/
Services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting Internet Safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss Internet Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

Parents/carers and pupils are actively encouraged to contribute to adjustments or reviews of the school Internet Safety policy by

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)
- Parents/carers are expected to sign a Home School agreement containing the following statement(s)
- I/we will support the school approach to online Internet Safety and not upload or add any text, image, sound or videos that could upset or offend any member of the school community, or bring the school name into disrepute.
- I/we will ensure that my/our online activity would not cause the school, staff, pupils or others distress or bring the school community into disrepute.
- I/we will support the school's policy and help prevent my/our child/children from signing up to services such as Facebook, Instagram, Snapchat and YouTube (edit/add services of particular concern here) whilst they are underage (13+ years in most cases).
- I/we will close online accounts if I/we/teachers find that these accounts are active for our underage child/children.

The school disseminates information to parents relating to Internet Safety where appropriate in the form of;

- Information evenings
- Practical training sessions e.g. current Internet Safety issues
- Posters
- School website information
- Newsletter items

Passwords and Password Security

Passwords

Please refer to the document on the grid for guidance: - 'how to Encrypt Files' which contains guidance on creating strong passwords and password security
http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

- **Always use your own** personal passwords
- Make sure you enter your personal passwords each time you log on. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- **Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else**. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- **Never tell a child or colleague your password**
- **If you aware of a breach of security with your password or account inform Lisa Rund immediately**
- Passwords must contain a minimum of six characters and be difficult to guess
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols
- User ID and passwords for staff and pupils who have left the school are removed from the system within ***6 months***

If you think your password may have been compromised or someone else has become aware of your password report this to Lisa Rund.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords, which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Internet Safety Policy and Data Security
- Pupils are not permitted to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers or others
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- Due consideration should be given when logging into the school learning platform, virtual learning environment or other online application to the

browser/cache options (shared or private computer)

- In our school, all ICT password policies are the responsibility of **Lisa Rund** and all staff and pupils are expected to comply with the policies at all times

Zombie Accounts

Zombie accounts refer to accounts belonging to all 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.

- 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

Personal or Sensitive Information

Protecting Personal or Sensitive Information

- 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 or sensitive 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 or sensitive information contained in documents you fax, copy, scan or print. This is particularly important when using shared copiers (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 or sensitive 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

Storing/Transferring Personal or Sensitive Information Using Removable Media

- Ensure removable media is purchased with encryption.
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Use Schools fx for data transfers or encrypt all files containing personal or sensitive data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean
- Please refer to the document on the grid for guidance on How to Encrypt Files http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

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
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- 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

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. HCC guidance can be found here: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

Please see photographic images policy for full details of use within our school.

Consent of Adults Who Work at the School

- Adults who work at the school make informed decisions as to whether they want to be in a photograph / video.
- At no time is there an expectation that they will be in a photograph or video
- It remains the responsibility of the adult to make the choice/ decision as and when the need arises

---

Publishing Pupil's Images and Work

- See Photographic consent form.

Storage of Images

- Images/ films of children are stored on the school's network and their personal EARWIG timeline
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource
- ***Terrianne Manning under the direction of Lisa Rund*** has the responsibility of deleting the images when they are no longer required, or when the pupil has left the school

Webcams and green screen use

- Webcams and green screen filming will not be used for broadcast on the internet without prior parental consent
- Misuse of the webcam / green screen by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)

- Notification is given in this/these area(s) filmed by webcams by signage
- Consent is sought from parents/carers and staff on joining the school, in the same way as for all images
- Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school
- All pupils are supervised by a member of staff when video conferencing
- The school keeps a record of video conferences, including date, time and participants
- Approval from the Headteacher is sought prior to all video conferences within school to end-points beyond the school
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
- No part of any video conference is recorded in any medium without the written consent of those taking part
- Additional points to consider:
- Participants in conferences offered by 3rd party organisations may not be DBS checked
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference
- For further information and guidance relating to Video Conferencing, please see

http://www.thegrid.org.uk/learning/ict/technologies/videoconferencing/index.shtml

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:
    - maintaining control of the allocation and transfer within their unit
    - recovering and returning equipment when no longer needed
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school network, and

not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use – but these must not be taken into classroom or any area of the school that a child is given access to.
- Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device unless there was an emergency situation.
- Pupils are not allowed to bring personal mobile devices/phones to school unless written consent has been given by the Governing body.
- This technology may be used for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed

- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school
- Never use a hand-held mobile phone whilst driving a vehicle

Telephone Services

You may make or receive personal telephone calls in designated places, provided:

- They are infrequent, kept as brief as possible and do not cause annoyance to others
- They are not for profit or to premium rate services
- They conform to this and other relevant school policies.
- They are not in lesson time

- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases
- Ensure that you are available to take any pre-planned incoming telephone calls
- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures are form part of the emergency plan and the information regarding the emergency plan is located in the school office.

Removable Media

If storing or transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section '**Storing/Transferring Personal or Sensitive Information Using Removable Media**'

- Always consider if an alternative solution already exists
- Only use recommended removable media
- Encrypt and password protect
- Store all removable media securely
- Removable media must be disposed of securely by Lisa Rund / Matthew Lee

Smile and Stay Safe Poster

Internet Safety guidelines to be displayed throughout the school

SMILE and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a ‘friend’

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

School Facebook account

The role of our Facebook account will be to:-

- Communicate informally and quickly with parents
- Share learning experiences with parents and carers
- Strengthen the connection between your home and our classroom
- Share news and information
- Share photos, videos and blogs of events
- Share the opportunities that we offer in school more widely
- Inform, engage and communicate with parents, carers and other interested parties.
- Recognise, celebrate and promote the work of the school and its students.
- Communicate and reinforce school policies and good practice.

Postings will include updates on school life, activities, clubs, events, useful information and websites, advice, suggestions, books and photos of activities.

Our school uses Facebook to communicate with parents and carers. All teaching staff and office staff are responsible for all postings on these technologies. We have set up the account so that no one can comment on the postings.

- Lisa Rund / Matthew Lee are ultimately responsible for monitoring posts

Guideline for posting

The Head Teacher / Governing Body will decide on and authorise administrators that will be responsible for updating the page on a regular basis. The administrators will communicate in a positive, accurate, respectful and responsible manner. They will uphold and promote the vision, mission statement and values of the school at all times.

- Parental consent must be gained in order to post picture of the children – staff must at all times adhere to this. Staff **must never** post a photograph of a child where parental support has not been gained.
- Children will not be named or described on the page or in comments on the page. This is due to data protection and the legal responsibility we have to keep the children safe.
- If followers have any specific concerns, particularly related to their own or other child/children, we ask them to speak directly to the Office Manager/Class teacher. In more serious cases the Head teacher / Governing Body
- All parents and carers are also welcome to like and share postings.

Administration

- The Governing body as part of their monitoring will regularly check the administration of the Facebook page and have set clear guidelines to all staff as follows:-
- Only authorised administrators have permission to upload photographs and videos on to the page. This is because they are aware of the parental permissions held by the school.
- No-one else is permitted to post any photographs or videos on to the page. The setting allowing people to post or tag photos will be turned off.
- No children will be tagged or named in relation to a photo directly on the page. However, there may be links to the school website or to third party articles (e.g. Blackpool Evening Gazette) where children may be photographed and/or named.

Site moderation

- The page will be moderated regularly by administrators that are authorised and by the Office Manager.
- It will be checked monthly by the SHE committee (governing body)
- All visitors to the page are asked to inform the Head Teacher / Governing Body or the school Office Manager of any concerns they have relating to the page.
- The page profanity filter will be set to ‘strong’.
- We encourage parents and carers to post regularly on the page by liking posts. There will be no facility to post comments.

Restrictions

- The page is designed as a communication tool to engage with parents and carers. It is therefore restricted to people over 18 years of age.
- Where a parent is under 18 years old, permission will be granted at the discretion of the Head Teacher / Governing body.
- The Head Teacher / Governing body also has the discretion to remove or ban any followers that are known to be under 18 years old.

Other policy guidelines linked Facebook accounts

- Staff ***are*** permitted to access their personal social media accounts using school equipment during breaks. However, this should be done in the staff work zones not the classrooms and staff must ensure that they log off.

- Staff are able to setup Social Learning Platform accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of Social Media

- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others

- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever

- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC
- Do not allow any unauthorized person to use school ICT facilities and services that have been provided to you
- Ensure you remove portable media from your computer when it is left unattended
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or HCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

Writing and Reviewing this Policy

Staff and Pupil Involvement in Policy Creation

Staff, governors and pupils have been involved in making/ reviewing the Policy for ICT Acceptable Use through:-

- **Staff meetings**
- **School council meetings**
- **Governor meetings**

Review Procedure

- There will be on-going opportunities for staff to discuss with the Internet Safety coordinator any Internet Safety issue that concerns them
- There will be on-going opportunities for staff to discuss with a member of SLT any issue of data security that concerns them
- This policy will be reviewed every (24) months and consideration will be given to the implications for future whole school development planning
- The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way
- This policy has been read, amended and approved by the staff, head teacher and governors on 20th December, 2016.

Further help and support

Your organisation has a legal obligation to protect sensitive information under the Data Protection Act 1998. For more information visit the website of the Information Commissioner's Office https://ico.org.uk/

Advice on Internet Safety - http://www.thegrid.org.uk/eservices/safety/index.shtml

Further guidance - http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

School's toolkit is available - Record Management Society website – http://www.rms-gb.org.uk/resources/848

Test your on linInternet Safety skills http://www.getsafeonline.org

Data Protection Team – email - data.protection@hertfordshire.gov.uk

Information Commissioner's Office – www.ico.org.uk

Cloud (Educational Apps) Software Services and the Data Protection Act – Departmental advice for local authorities, school leaders, school staff and governing bodies, October 2015. This is an advice and information document issued by the Department for Education. The advice is non-statutory, and has been produced to help recipients understand some of the key principles and their obligations and duties in relation to the Data Protection Act 1998 (the DPA), particularly when considering moving some or all of their software services to internet-based "cloud" service provision –

https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

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 Internet Safety

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 (email) 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 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/

Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation & Counter-Extremism Guidance

https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services

Appendix

School Policy in Brief

- At this school we have an Acceptable Use policy which is reviewed at least annually, which all staff signs. Copies are kept on file. .
- ICT Acceptable Use Agreements are signed by all Staff/Governors/Students/Visitors. We use the Herefordshire LA model agreements.
- Safe Handling of Data Guidance documents are issued to all members of the school who have access to sensitive or personal data.

Personal or sensitive material must be encrypted if the material is to be removed from the school

- At this school we encrypt flash drives / use automatically encrypted flash drives> for this purpose and limit such data removal.
- At this school we use Lancashire Secure email facilities to securely transfer CTF pupil data files to other schools.
- At this school we follow LA guidelines for the transfer of any other internal data transfer, using <Outlook> <secure export to Local Authority Pupil Database>.

Personal or sensitive material must be held in a lockable storage area or cabinet if in an un-encrypted format (such as paper)

- At this school we store such material in lockable storage cabinets in a lockable storage area.
- At this school all servers are in lockable locations and managed by CRB-checked staff.
- At this school we use Westfield for disaster recovery on our admin server.

Disposal: personal or sensitive material electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.

- At this school paper based sensitive information is shredded
- Laptops used by staff at home (loaned by the school) where used for any protected data are brought in and disposed of through the same procedure.

- Security policies are reviewed and staff updated at least annually and staff know to whom they should report any incidents where data protection may have been compromised. Staff have guidance documentation.