"Nurturing Life-Long Learning"

Online & Data Security

Adopted by Governing Body:	November 2023
Review Date:	November 2024

All the policies of Morgans Nursery and Primary School reflect the aims and values of the school.

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

CONTENTS

Introduction

Computing and 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. 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
- Online 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 Computer Science and 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 **Morgans 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).

Please also refer to the Online Safety Policy

Monitoring

Authorised tech staff may inspect any 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 for their identification badge and contact their department. Any authorised tech staff member will be happy to comply with this request.

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

Authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by 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 technologies may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

In addition, all internet activity is logged by the school's internet provider. These logs may be monitored by that provider (eg Herts for Learning Ltd).

Breaches

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

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

Policy breaches may also lead to criminal or civil proceedings.

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

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

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

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 technology must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of technologies and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individual in the school is Mrs Helen Melidoro, Head Teacher.

Please refer to the relevant section on Incident Reporting, Online Safety Incident Log & Infringements.

Morgans Primary Pupil Acceptable Use Agreement / Online Safety Rules

Please refer to the Online Safety Policy

Acceptable Use Agreement: Staff, Governors and Visitors

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

Please refer to the Online Safety Policy.

Staff Professional Responsibilities

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

PROFESSIONAL RESPONSIBILITIES

When using any form of ICT, including the Internet, in school and outside school

For your own protection we advise that you:

- 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 YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.
- Do not give out your own personal details, such as 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/ or 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 online activity, **both in school and outside school**, will not bring your organisation or professional role into disrepute.

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

For HR support and guidance please contact 01438 844933
For eSafety support and guidance please contact 01438 844893

Computer Viruses

- All files downloaded from the Internet, received via e-mail 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 equipment.

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

- If you suspect there may be a virus on any school equipment, stop using the equipment and contact your tech support provider immediately. The tech support provider will advise you what actions to take and be responsible for advising others that need to know. Morgans IT service provider is Technology In Schools - Herts for Learning.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

The Local Authority guidance documents listed below

HGfL: School Admin: School Office: Data Protection and Freedom of Information

- Headteacher's Guidance – Data Security in Schools – Dos and Don'ts
- Network Manager/MIS Administrator or Manager Guidance – Data Security in Schools
- Staff Guidance – Data Security in Schools – Dos and Don'ts
- Data Security in Schools - Dos and Don'ts

Refer to Online Safety Policy

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 Acceptable Use.
- Staff have read the relevant guidance documents available on the SITSS website concerning 'Safe Handling of Data' (available on the grid at - http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata)
- Leadership have identified relevant responsible persons as defined in the guidance documents on the SITSS website (available - http://www.thegrid.org.uk/info/traded/sitss/)
- Staff keep 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, sensitive, confidential and classified information contained in documents faxed,

copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used

- Anyone sending a confidential or sensitive online message should check it with their line manager or a colleague before it is sent and notify the Head Teacher.

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 should be familiar with information risks and the school's response. Previously called a Senior Information Risk Officer (SIRO), there should be a member of the senior leadership team who 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

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 Equipment Policy

- All redundant 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 eg 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

e-mail

Refer to Online Safety Policy

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

Managing e-mail

- The school gives all staff & governors their own e-mail account to use for all school business as a work based tool. This is to protect staff and governors, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
- Staff & governors should only use their school email for professional communication or relating to Morgans Primary School.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Head Teacher, or the Business Manager, as appropriate, depending upon the relevance of the email.
- Pupils may only use school approved accounts on the school system and only under direct teacher / Assistant Teacher supervision for educational purposes
- E-mails 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 e-mail account as follows:

- Delete all e-mails of short-term value
- Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

- All children use a class/ group e-mail address
- The forwarding of chain emails is not permitted in school unless the school has set up a dummy account to allow pupils to forward any chain emails causing them anxiety. No action will be taken with this account by any member of the school community
- All pupil e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail
- Staff must inform (the Online Safety co-ordinator or line manager) if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the Computing Programme of Study
- However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply
- The linking of any school e-mail account to a personal e-mail address by use of an e-mail forwarder is prohibited.

Sending e-mails

- If sending e-mails 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 e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of e-mail 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 e-mail is not to be used for personal advertising

Receiving e-mails

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

e-mailing SLT

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

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

  - Encrypt and password protect. See http://www.thegrid.org.uk/info/dataprotection/#securedata
  - Verify the details, including accurate e-mail address, of any intended recipient of the information
  - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
  - Do not copy or forward the e-mail to any more recipients than is absolutely necessary

  - Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
  - Send the information as an encrypted document **attached** to an e-mail
  - Provide the encryption key or password by a **separate** contact with the recipient(s)
  - Do not identify such information in the subject line of any e-mail

- Request confirmation of safe receipt

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' Online Safety rules.

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

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Online 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 Online Safety co-ordinator in this school is **Mrs Tina Taylor and Mrs.Helen Melidoro** who has been designated this role as Head teacher. All members of the school community have been made aware of who holds this post. It is the role of the Online Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Herts LA, Herts for Learning Ltd, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the Head/ Online Safety Co-ordinator 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.

Online Safety in the Curriculum

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

- The school has a framework for teaching skills in Computing/ICT/ PSHE lessons and guidlelines and follows the NCCE Scheme of work.
- The school provides opportunities within a range of curriculum areas to teach about Online Safety
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the Online 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, modelling 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 Cybermentors, Childline or CEOP report abuse button

- Pupils are taught critically to evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum, *PSHCE units and Scheme of works.*

Online Safety Skills Development for Staff

- Our staff receive regular information and training on Online Safety and how they can promote the 'Stay Safe' online messages in the form of regular bulletins, staff meetings and emails from Mrs. Helen Melidoro, Head Teacher, Business Manager and Online Safety Coordinator.

- Details of the ongoing staff training programme can be obtained from Mrs. Helen Melidoro, the Head Teacher, Business Manager and Online Safety Coordinator.

- New staff receive information on the school's acceptable use policy as part of their induction

- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community (see Online Safety Co-ordinator)

- All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

Managing the School Online Safety Messages

- We endeavour to embed Online Safety messages across the curriculum whenever the internet and/or related technologies are used

- The Online Safety policy (AUP) will be introduced to the pupils at the start of each school year or on intake.

- Online Safety posters will be prominently displayed

- The key Online Safety advice will be promoted widely through school displays, newsletters, class activities and so on

- We will participate in Safer Internet Day every February.

Incident Reporting, Online Safety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of equipment must be immediately reported to Mrs. Helen Melidoro, head teacher or Online Safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Information Asset Owner.

The DPO is Mr Richard Maskrey. Detail available on request.

Online Safety Incident Log

Keeping an incident log can be a good way of monitoring what is happening and identify trends or specific concerns.

Please refer to the Online Safety Policy.

Misuse and Infringements

Complaints

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

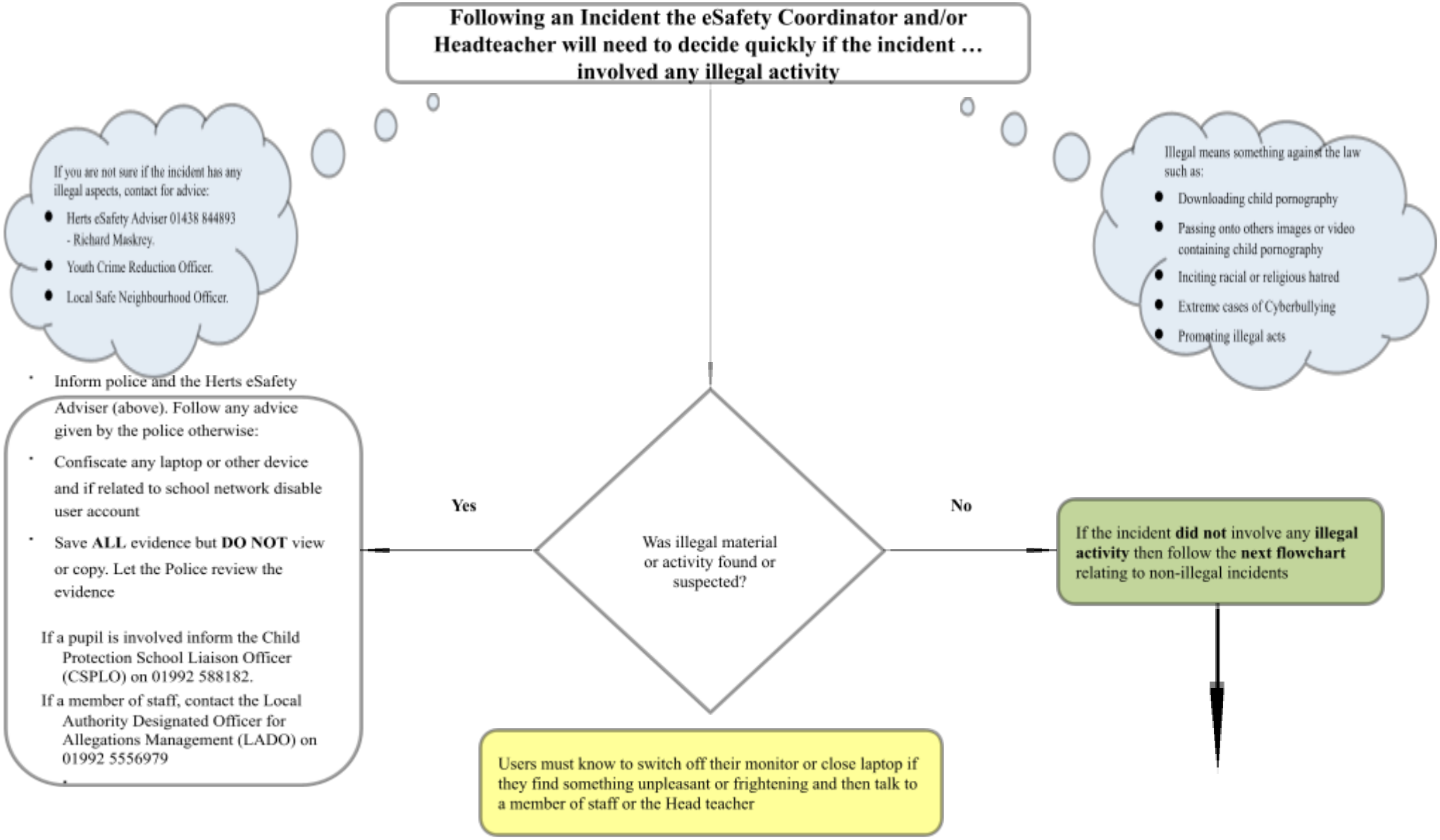
Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Headteacher or Online 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 Headteacher / Online Safety coordinator. 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 school's behaviour policy.)

Flowcharts for Managing an Online Safety Incident

These three flowcharts have been developed by the HSCB Online Safety subgroup and are designed to help schools successfully manage Online Safety incidents
http://www.thegrid.org.uk/eservices/safety/incident.shtml

Hertfordshire Flowchart to support decisions related to an illegal Online Safety Incident
For Headteachers, Senior Leaders and Online Safety Coordinators



ertfordshire Managing an Online Safety Incident Flowchart

For Headteachers, Senior Leaders and Online Safety Coordinators

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

The eSafety Coordinator and/ or Headteacher should:

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

Incident could be:

- Using another person's user name and password
- Accessing websites which are against school policy e.g. games, social networks
- Using a mobile phone to take video during a lesson
- Using the technology to upset or bully (in extreme cases could be illegal) – talk to Herts. Anti-Bullying Adviser Karin Hutchinson 01438 844767

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 on: **01992 556979** If the incident **does not** satisfy the criteria in **10.1.1** of the **HSCB procedures 2007**, then follow the bullet points below:

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

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
- eSafety 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 CSPLO immediately

Confiscate the device, if appropriate.

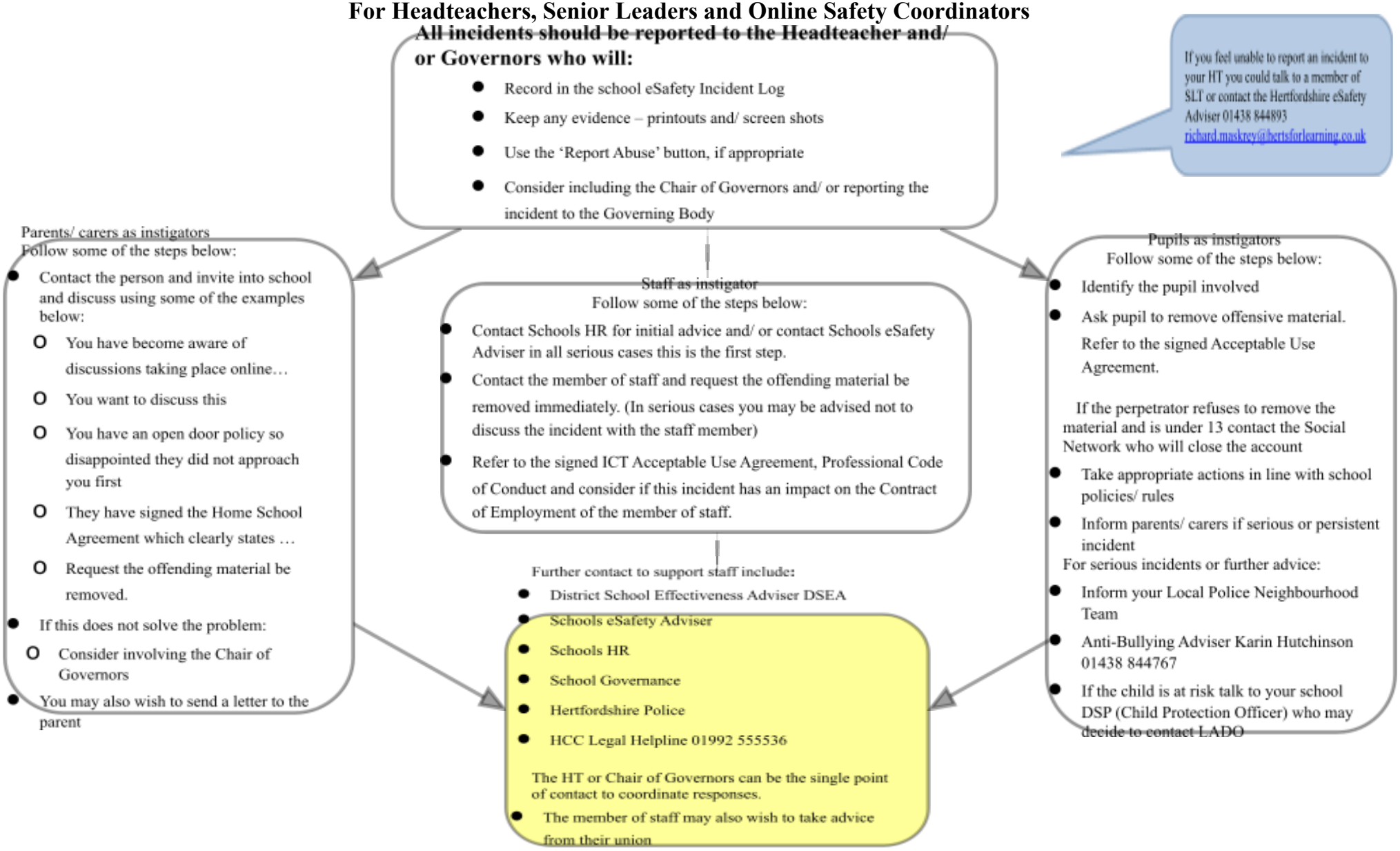
Pupil as instigator

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

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the Head teacher.

Hertfordshire Managing an Online Safety Incident Flowchart involving staff as victims

For Headteachers, Senior Leaders and Online Safety Coordinators



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 HICS network (Hertfordshire Internet Connectivity Service) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

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

- You must not post Personal or Confidential Information or disseminate such information in any way that may compromise the intended restricted audience
- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application
- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- Hertfordshire Local Authority has a monitoring solution via the Hertfordshire Grid for Learning where web-based activity is monitored and recorded

- School internet access is controlled through the HICS web filtering service. For further information relating to filtering please go to http://www.thegrid.org.uk/eservices/safety/filtered.shtml

- Our school also employs some additional web-filtering which is the responsibility of **SITTS / HICS**

- Morgans Primary 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

- The school does not allow pupils access to internet logs

- The school uses management control tools for controlling and monitoring workstations

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the Online-Safety coordinator or teacher as appropriate

- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines

- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the ***Headteacher*** / Online Safety Coordinator for a safety check first

- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the OnlineSafety coordinator / Headteacher.

- If there are any issues related to viruses or anti-virus software, SITTS should be informed as soon as possible. This is communicated by the teachers and school office by telephone/ Service Desk On-Line or email directly with SITTS.

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 denies access to social networking and non educational online games and websites to pupils within school
- Out of 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, WhatsApp 16 + 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 Online Safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss Online 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 Online Safety policy by school newsletters and information evenings.

- Parents/carers are asked to read through acceptable use agreements on behalf of their child on admission to the school and at the start of every academic year.

- 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 (eg, on school website)

- Parents/carers are expected to sign a Home School agreement containing the following statement or similar:

  > " Protect all children from the dangers of social networking sites and innappropriate Apps and games and supervise internet use"

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

  - Information evenings
  - Practical training sessions eg current Online Safety issues
  - Posters
  - School website information
  - Newsletter items/emails

Passwords and Password Security

Passwords

Please refer to the document on the grid for guidance on 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 login. Do not include passwords in any automated logon procedures
- Staff and governors should change temporary passwords at first login
- 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 Tech 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 the Online Safety coordinator Mrs. Helen Melidoro or Mrs Tina Taylor 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, governors and pupils who have left the school are removed from the system as soon as practically possible.

If you think your password may have been compromised or someone else has become aware of your password, report this to your Tech support team and/or SITTS(UK) Ltd.

Password Security

Password security is essential for staff and governors. Staff are able to access and use pupil data and governors may receive confidential information via their school e-mail account.. Staff and governors 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, governors 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 Online-Safety Policy and Data Security
- Users are provided with an individual network, email and Management Information System log-in username. They are also expected to use a personal password and keep it private
- Pupils are not allowed 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. The automatic log-off time for the school network will be advised to individual users.
- 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 password policies are the responsibility of Mrs. Helen Melidoro and Mrs Taylor and all staff, governors and pupils are expected to comply with the policies at all times

Zombie Accounts

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

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

Personal or Sensitive Information

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

Storing/Transferring Personal or Confidential Information Using Removable Media

- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified 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, eg 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:
http://www.thegrid.org.uk/eservices/safety/research/index.shtml#safeuse

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

Consent of Adults Who Work at the School

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

Publishing Pupil's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos/videos in the following ways:

- on the school web site
- school production
- school trips
- in the school prospectus and other printed publications that the school may produce for promotional purposes -school photography companies.
- recorded/ transmitted on a video or webcam
- training materials
- on the school's learning platform or Virtual Learning Environment

- in display material that may be used in the school's communal areas

- in display material that may be used in external areas, ie exhibition promoting the school

- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

All staff and the Chair of Governors have authority to upload to the school website.

For further information relating to issues associated with school websites and the safe use of images in Hertfordshire schools, see

http://www.thegrid.org.uk/schoolweb/safety/index.shtml
http://www.thegrid.org.uk/info/csf/policies/index.shtml#images

---

Storage of Images

Please refer to the Online Safety Policy.

Webcams and CCTV

- The school does not currently use CCTV for security and safety.

- We do use publicly accessible webcams in school and ensure chromebook cameras are off when not in direct use.

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

School Equipment

- As a user of the school equipment, you are responsible for your activity
- It is recommended that schools log equipment issued to staff and record serial numbers as part of the school's inventory
- Visitors are only permitted to plug their hardware into the school network points (unless special provision has been made) under the supervision of a member of the senior management team. They should be directed to the wireless facilities if available
- Ensure that all 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 - as a google school to store on shared drives.
- 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 equipment should not be used on a school network.
- On termination of employment, resignation or transfer, return all equipment to your Headteacher. 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 or Confidential Information is disclosed to any unauthorised person
- All 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 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 as laptops, chromebooks and iPads 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)

Please also refer to the Online Safety Policy.

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device, except in the case of emergency contact when the school mobile is not available. It is recommended that in such circumstances the staff member should advise another member of staff of her actions, if possible.

- Pupils are not allowed to bring personal mobile devices/phones to school without prior consent of Mrs. Helen Melidoro, Headteacher, and only in exceptional circumstances. Any mobile device brought into school under these conditions must be handed into the School Office for safe keeping during the day and collected at the end of school. This technology may be used for educational purposes by the teaching staff only. 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, chromebooks and iPads for off site visits and trips, only these devices should be used

- Where the school provides a laptop, chromebook or iPad 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 provided:

    1. They are infrequent, kept as brief as possible and do not cause annoyance to others

    2. They are not for profit or to premium rate services

    3. They conform to this and other relevant HCC and school policies.

- 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 your incoming telephone calls can be handled at all times

- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask the Business Manager.

Removable Media

If storing or transferring Personal or Confidential Information using Removable Media please refer to the section '**Storing/Transferring Personal or Confidential Information Using Removable Media**'

- Always consider if an alternative solution already exists
- Only use encrypted removable media
- Encrypt and password protect
- Store all removable media securely
- Removable media must be disposed of securely by your tech support team

Servers

- Always keep servers in a locked and secure environment
- Limit access rights
- Always password protect and lock the server
- Existing servers should have security software installed appropriate to the machine's specification
- Data is backed up daily as well as being remotely backed up by SITTS.
- Back up media stored off-site must be secure
- Remote backups should be automatically securely encrypted. SITSS provide an encrypted remote back up service. Please contact the SITSS helpdesk for further information – 01438 844777
- Newly installed Office Master PCs acting as servers and holding personal data should be encrypted, therefore password protecting data. At the moment SITSS do not encrypt servers, however Office PCs (including Office Master PCs) installed by SITSS are supplied with encryption software installed

Smile and Stay Safe Poster

Online Safety guidelines to be displayed throughout the school

and stay safe

SMILE 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, Instagram and Twitter

Facebook is used in the school environment, by staff only.

Morgans Primary School has a Facebook account which it uses to share news with the school community.

Only authorised staff have access and are responsible for setting up, managing and monitoring Morgans Primary School social media pages.

The named person for this is……..

To ensure all social media content has a purpose and a benefit and accurately reflects the school ethos and values.

To deal with any issues in connection with the social media accounts.

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.
- Do not allow any unauthorised 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 or Confidential 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 log off from the device completely when you are going to be away from the 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 a 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 repeatedly overwriting the data.

Writing and Reviewing this Policy

Staff and Pupil Involvement in Policy Creation

- Staff, and governors have been involved in making/ reviewing the Policy for ICT Acceptable Use through review meetings between staff and governors.

Review Procedure

There will be on-going opportunities for staff to discuss with the Online Safety coordinator any Online Safety issue that concerns them

There will be on-going opportunities for staff to discuss with the SLT any issue of data security that concerns them

This policy will be reviewed every 12 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.

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 Online 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 online 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 2014. 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/uploads/system/uploads/attachment_data/file/404098/Cloud-services-software-dept-advice-Feb_15.pdf

For additional help, email school.ictsupport@education.gsi.gov.uk

Current Legislation

Acts Relating to Monitoring of Staff email

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

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

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to eSafety

Racial and Religious Hatred Act 2006

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

Sexual Offences Act 2003

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

Communications Act 2003 (section 127)

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

The Computer Misuse Act 1990 (sections 1 – 3)

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

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

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

Malicious Communications Act 1988 (section 1)

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

Copyright, Design and Patents Act 1988

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

Public Order Act 1986 (sections 17 – 29)

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

Protection of Children Act 1978 (Section 1)

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

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

Appendix 1

At Morgans Primary School we have overall strategic responsibility for filtering and monitoring.

To do this we:

Have appointed members of the senior leadership team and the Online Safety Coordinator. Mrs Tina Taylor to be responsible for ensuring these standards are met.

Technical requirements to meet the standard

We are responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your provision
- overseeing reports

We are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

Senior leaders work closely with governors, the Online Safety Coordinator, the designated safeguarding lead (DSL) and IT service - Interim IT & HFL in all aspects of filtering and monitoring.

Day to day management of filtering and monitoring systems requires specialist knowledge of both safeguarding and IT staff to be effective. The DS, and OSC work closely together with IT service providers to meet the needs of your setting.

The DSL and OSC takes lead responsibility for safeguarding and online safety, which could include overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

Interm IT & HFL have technical responsibility for:

- maintaining filtering and monitoring systems

- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

Interm IT & HFL work with the senior leadership team, the OSC and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

Our Filtering is set by HFL and we operate a WF1 filtering system for staff and a WF3 filtering system for children.

We use Senso as our monitoring system and this is checked each evening.