



**St Albert the Great Catholic Primary School**  
*"The more I learn about the world in which I live the closer I grow to God"*



## **E- Safety Policy**

### **The Catholic Ethos of the School**

At St. Albert the Great Catholic Primary School we aim to provide the highest quality education and care for all our children. We aim to offer a welcome to each child and family and to provide a warm, caring and safe environment within which all children can learn and develop.

Our school was founded by and is part of the Catholic Church. The school is to be conducted as a Catholic school in accordance with canon law and teachings of the Catholic Church, and in accordance with the Trust Deed of the Archdiocese of Westminster and at all times the school is to serve as a witness to the Catholic faith in Our Lord Jesus Christ.

It is thus the responsibility of all members of the school, pupils, parents and teachers, to take swift and appropriate action when relationships in our community conspicuously fail to reflect these ideals. The following policy is commended as a series of concrete courses of action to assist in this endeavour.

### **Introduction**

ICT in the 21<sup>st</sup> 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, we need to build in the use of these technologies in order to arm our pupils 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.

At St Albert the Great school, we understand the responsibility to educate our pupils on eSafety 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.

St Albert the Great school holds personal data on learners, staff and other people so that their day-to-day activities can be carried out. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual.

Everybody in St Albert the Great school 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 are aware of the risks and threats and how to minimise them.

This policy is inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, 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, camera phones, PDAs and portable media players, etc).

Staff, pupils and Governors have been involved in the creation of this policy through staff meetings, ICT lessons, Pupil Council and full Governing Body meetings.

### **Monitoring**

The Headteacher or Deputy Headteacher may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving the schools 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.

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 an employee, contractor or pupil may result in the temporary

or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure and may lead to criminal or civil proceedings

The Information Commissioner's Office's (ICO) new 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.

### **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 Headteacher or Deputy Headteacher in her absence. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Headteacher or Deputy Headteacher.

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

### **Computer Viruses**

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. floppy disk, CD) must be checked for any viruses using school provided anti-virus software before using them
- Never interfere with any anti-virus software installed on school ICT equipment that you use
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates in liaison with Martin Weatherilt @ ConEd
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact Martin Weatherilt @ConEd immediately who will advise you what actions to take and be responsible for advising others that need to know

### **Data Security**

The accessing and appropriate use of school data is something that is taken very seriously at our school.

Our school follows Becta guidelines [Becta Schools - Leadership and management - Security - Data handling security guidance for schools](#) (published Spring 2009) and 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
- SIRO/IAO Guidance – Data Security in Schools - Dos and Don'ts
- The School gives relevant staff access to its Management Information System, with a unique ID 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
- 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/traded/sitss/>)
- Leadership have identified Senior Information Risk Owner (SIRO) and Asset Information Owner(s) (AIO) 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 their 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 copiers (multi-function print, fax, scan and copiers) are used
- Anyone expecting a confidential/sensitive fax, should warn the sender to notify before it is sent.

### **Impact Levels and Protective Marking**

Appropriate labelling of data helps the school secure data and so reduce the risk of security incidents.

Labelling is applied in accordance with guidance from the Senior Information Risk Owner (SIRO)

Most learner or staff personal data will be classed as 'Protect' e.g. PROTECT – PERSONAL e.g. personal information about an individual, PROTECT – STAFF e.g. Organisational staff only

### **Senior Information Risk Owner (SIRO)**

At St Albert the Great school the SIRO is the Head teacher and has the following responsibilities:

- they own the information risk policy and risk assessment
- they appoint the Information Asset Owner(s) (IAOs)
- they act as an advocate for information risk management

### **Information Asset Owner (IAO)**

Any information that is sensitive needs to be protected. This includes the personal data of learners and staff; such as assessment records, medical information and special educational needs data. Appendix D shows examples of information assets St. Albert the Great Primary School holds. In our school the IAO is the Headteacher.

The role of the IAO is to understand:

- what information is held, and for what purposes
- what information needs to be protected (e.g. any data that can be linked to an individual, pupil or staff etc including UPN, teacher DCSF number etc)
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed off

Although these roles have been explicitly identified, the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action

### **Disposal of Redundant ICT Equipment**

All redundant ICT equipment is disposed off through an authorised agency or via the Hertfordshire Business Services (HBS) disposal scheme.

Disposal of any ICT equipment conforms to:

- The Waste Electrical and Electronic Equipment Regulations 2006
- The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
- Data Protection Act 1998
- Electricity at Work Regulations 1989

St Albert the Great Catholic Primary School maintains a comprehensive inventory of all its ICT equipment including a record of its disposal.

### **E-mail**

The use of e-mail within our school is an essential means of communication for both staff and pupils. In the context of school, e-mail is not considered private. We recognise that pupils need to understand how to style an e-mail in relation to their age and good 'network etiquette'; 'netiquette'. In order to achieve ICT level 4 or above, pupils are given the opportunity to send and receive e-mails.

### **Managing E-mail**

- The school gives all staff their own e-mail account to use for **all** school business as a work based tool
- 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 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

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette 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 e-mail
- Staff must inform the Headteacher if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the ICT Scheme of Work
- However school e-mails are accessed (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

### **Sending E-mails**

- Always 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
- An outgoing e-mail greater than ten megabytes (including any attachments) is likely to be stopped automatically. This size limit also applies to incoming e-mail

### **Receiving E-mails**

- Check your e-mail regularly
- Never open attachments from an untrusted source; Consult your network manager first.

### **E-mailing Personal, Sensitive, Confidential or Classified Information**

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted
- Where your conclusion is that e-mail must be used to transmit such data:
  - Obtain express consent from the Headteacher to provide the information by e-mail
  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
    - o Verify the details, including accurate e-mail address, of any intended recipient of the information
    - o Verify (by phoning) the details of a requestor before responding to e-mail requests for information
    - o Do not copy or forward the e-mail to any more recipients than is absolutely necessary
  - Do not send the information to any body/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

In exceptional circumstances, the County Council makes provision for secure data transfers to specific external agencies. Such arrangements are currently in place with:

- Hertfordshire Constabulary
- Hertfordshire Partnership Trust

### **Equal Opportunities**

At St. Albert the Great School we endeavour to create a consistent message with parents for all

pupils. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children.

### **E-Safety**

#### **E-safety – Roles and Responsibilities**

As E-safety is an important aspect of strategic leadership within our school, the Head and governors are responsible for ensuring that the policy and practices are embedded and monitored. The named E-safety co-ordinator in this school the Headteacher. The E-safety co-ordinator keeps abreast of current issues and guidance through organisations such as Herts LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Headteacher and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

#### **E-safety in the Curriculum**

ICT and online resources are increasingly used across the curriculum. At St. Albert the Great School we believe it is essential for E-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote E-safety.

E-safety posters are prominently displayed throughout our school.

#### **E-safety Skills Development for Staff**

New staff receive information on our school's acceptable use of ICT as part of their induction and all staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

#### **Managing an E-safety Incident**

At St. Albert the Great School we follow the recommended Hertfordshire flowchart to support decisions related to illegal safety incidents. (Appendix D)

#### **E-safety Incident Reporting**

Incidents are recorded on the Incident log (Appendix E) which is kept in the Incidents File in the Headteacher's office.

Some incidents may need to be recorded in other places, such as Solero, if they relate to a bullying or racist incident.

#### **Internet Access**

##### **Managing the Internet**

In the interest of safety staff always preview any recommended sites before use. If Internet research is set for homework, specific sites, which have previously been checked by the teacher, are suggested. Parents recheck these sites and supervise this work. Parents are advised to supervise any further research the children carry out

All users observe copyright of materials from electronic resources

##### **Internet Use**

Colleagues' or pupils' names or any other confidential information is not to be revealed on any social networking site or blog While on-line gambling or gaming is not allowed.

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

##### **Infrastructure**

At St. Albert the Great School we use a monitoring solution via the Hertfordshire Grid for Learning where web-based activity is monitored and recorded. School internet access is controlled through the LA's

web filtering service. For further information relating to filtering please go to <http://www.thegrid.org.uk/eservices/safety/filtered.shtml>

If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the teacher or Headteacher. Martin Weatherill of Con-Ed ensures that Anti-virus protection is installed and kept up-to-date on all school machines. If there are any issues related to viruses or anti-virus software, he should be immediately informed by mobile phone. Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Headteacher.

At present, the school endeavors to deny access to social networking sites to pupils within school.

### **Parental Involvement**

At St. Albert the Great School we believe that it is essential for parents/ carers to be fully involved with promoting E-safety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss E-safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

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

- **We will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community**

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

- Posters
- Newsletter items

### **Passwords and Password Security**

Staff always use their own personal passwords to access computer based services and no passwords are included in any automated logon procedures. Temporary passwords are changed at the first logon. Passwords or encryption keys are not recorded on paper or in unprotected files.

Staff are reminded to only disclose their personal passwords to authorised ICT support staff when necessary, and never to anyone else. Any passwords must contain a minimum of six characters and be difficult to guess and User ID and passwords for staff and pupils who have left the School are removed from the system within 12 months.

*If you think your password may have been compromised or someone else has become aware of your password speak to the Headteacher.*

### **Protecting Personal, Sensitive, Confidential and Classified Information**

All staff ensure that screens are locked before moving away from their computers to prevent unauthorised access and screen displays are kept out of direct view of any third parties when staff are accessing personal, sensitive, confidential or classified information

Measures are taken to 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 copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment.

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

Removable media for school use is purchased with encryption and stored securely in the store cupboard at school. All removable media that may hold personal data is securely disposed of and all hard drives from machines no longer in service are removed and stored securely or wiped clean

### **Remote Access**

At St Albert the Great school we are responsible for all activity via the remote access facility and for this reason we only use equipment with an appropriate level of security for remote access.

PINs are selected to ensure that they are not easily guessed and School information and data, including any

printed material produced while using the remote access facility is protected at all times. We take particular care when access is from a non-School environment.

### **Safe Use of Images**

#### **Taking of Images and Film**

Staff and pupils 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.

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 and Storing Pupils' Images and Work**

At St. Albert the Great School written consent of parents is required for images to be taken with school equipment when a child joins the school. Parents / carers are asked to give permission for their child's work / photos to be used in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- 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 is considered valid for the entire period that the child attends St. Albert the Great School unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc and parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names are not published alongside their image and vice versa. E-mail and postal addresses of pupils are never published. Pupils' full names are not published.

Images/ films of children are stored on the school's network and 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.

#### **Webcams and CCTV**

The school uses CCTV for security and safety. The only people with access to this are the Headteacher and administration staff. Notification of CCTV use is displayed at the front of the school.

We do not use publicly accessible webcams in school

#### **School ICT Equipment including Portable and Mobile ICT Equipment and Removable Media**

##### **School ICT Equipment**

All ICT equipment issued to staff is logged in the school's inventory and serial numbers are recorded. On termination of employment, resignation or transfer, all ICT equipment should be returned to the Headteacher along with details of their system logons so that they can be disabled.

Staff are responsible for any activity undertaken on the school's ICT equipment provided to them and responsible for its security. They are advised to save their data on a frequent basis to the school's network drive as they are responsible for the backup and restoration of any of data that is not held on the school's network drive.

Staff do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data as this is an offence under the Computer Misuse Act 1990.

Visitors are not permitted to plug their ICT hardware into the school network points (unless special provision has been made) and are directed to the wireless ICT Facilities if necessary.

### **Personal Mobile Devices and school provided devices (including phones)**

At St. Albert the Great Primary School staff are permitted to bring in personal mobile phones and devices for their own use. However, these devices must not be used during lesson time or in front of parents or children. Staff are also urged to consider social etiquette when using their personal mobile devices. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device. The school is not responsible for the loss, damage or theft of any personal mobile device.

Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device and permission must be sought before any image or sound recordings are made on these devices of any member of the school community

Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used for school business.

### **The School Server**

The school server is in a locked and secure environment and access rights are limited. A password is used to protect and lock the server for security reasons and back up tapes are encrypted using appropriate software. Data is backed up daily.

### **Systems and Access**

Staff should only use their own personal logons, account IDs and passwords and must not allow them to be used by anyone else. All staff are responsible for all activity on school systems carried out under any access/account rights assigned to them, whether accessed via school ICT equipment or their own PC. It is imperative that staff do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, 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)

Where necessary, permission is obtained from the owner or owning authority and any relevant fees are paid before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998

Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act

### **Telephone Services**

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.

### **Mobile Phones**

Staff are responsible for the security of the school mobile phone. The PIN code must always be set and the phone must not be left unattended and on display (especially in vehicles). Loss or theft of the school mobile phone equipment must be reported immediately as the school remains responsible for all call costs until the phone is reported lost or stolen.

The school's own SIM card must only be used in the school's mobile phone and the phone is barred from calling premium rate numbers and any numbers outside of the UK as the default.

In accordance with the Finance policy on the private use of School provided mobiles, staff must reimburse the school for the cost of any personal use of the school mobile phone. This includes call charges incurred for incoming calls whilst abroad. To assist staff identifying personal use, they should add \* to the end of the number being contacted, this will enable the number to be shown separately on the bill. Payment arrangements should be made with Angela Langley, the school's financial secretary.

Staff are reminded never to use a hand-held mobile phone whilst driving a vehicle. Only genuine 999 or 112 emergency calls may be made if it would be unsafe to stop before doing so.

**Review Procedure**

There will be an on-going opportunity for staff, pupils, governors or parents to discuss with the Headteacher any issue of eSafety or data security that concerns them.

This policy will be reviewed annually and consideration given to the implications for future whole school development planning

**Date approved:****Date for Review:****Acknowledgements:**

- SSE, Herts. CSF ICT Team
- Becta
- Cabinet Office
- Information Commissioners Office
- Record Management Society

Draft

# Appendix A

## Pupil eSafety Rules



- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.
- We will support the school approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the school community

Signed: \_\_\_\_\_ Date: \_\_\_\_\_

# Appendix B



**St Albert the Great Catholic Primary School**  
Acorn Road, Bennetts End, Hemel Hempstead, Hertfordshire, HP3 8DW  
Tel: 01442 264835 e-mail: [admin@albertthegreat.herts.sch.uk](mailto:admin@albertthegreat.herts.sch.uk)



*"The more I learn about the world in which I live the closer I grow to God"*

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies, has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mrs Anderton or Mrs Fleming.

We thank you for your support.

✂

**Parent/ carer signature**

We have discussed this and .....(child name) agrees to follow the eSafety rules and to support the safe use of ICT at St Albert the Great School.

Parent/ Carer Signature .....

Class ..... Date .....

# Appendix C

## e-Safety and Acceptable Use Agreement: Staff, Governors and Visitors



ICT (including data) and the related technologies such as e-mail, 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 the Headteacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' 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 and personal e-mail address, to pupils or parents.
- I will only use the approved, secure e-mail system 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.
- I will not install any hardware or software without permission of the Headteacher.
- 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 inline 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 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 the Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

### **User Signature**

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

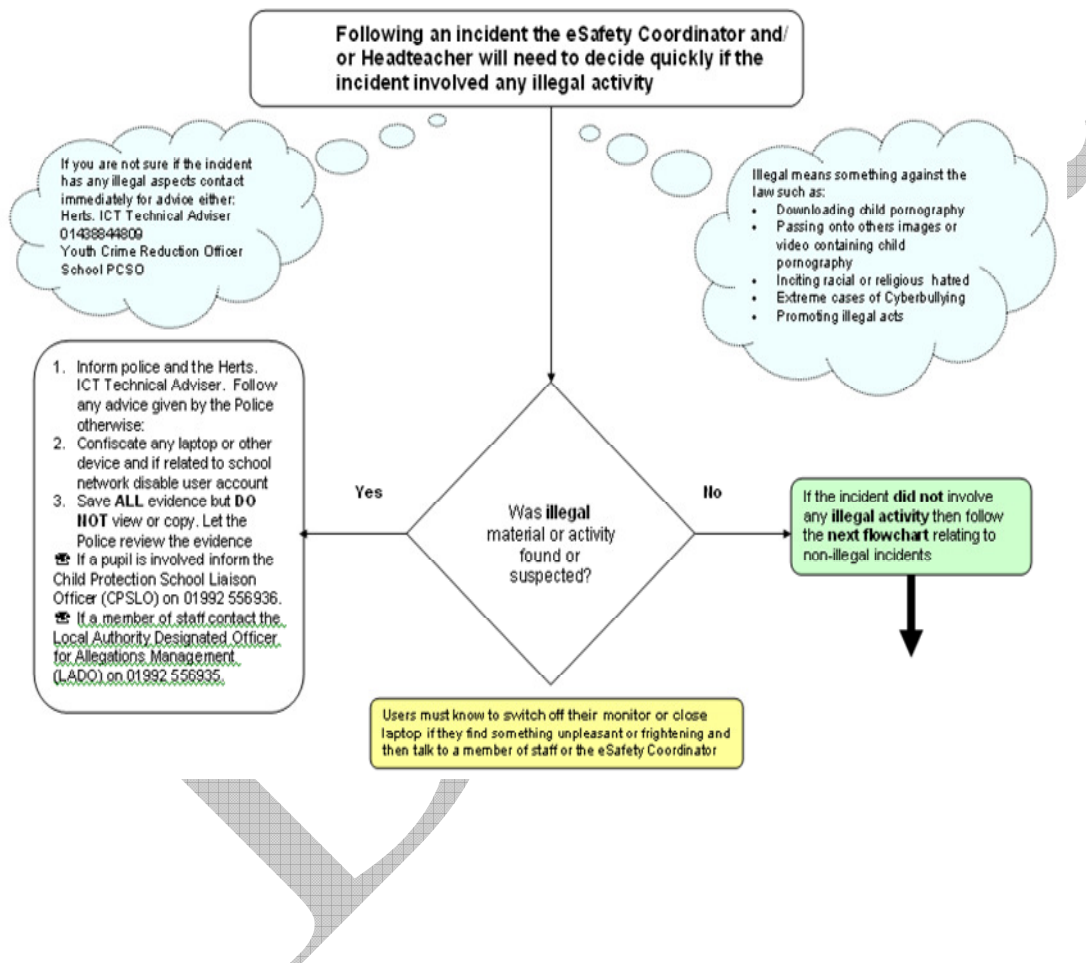
Signature ..... Date .....

Full Name ..... (printed)

Job title .....

# Appendix D

Hertfordshire Flowchart to support decisions related to an Illegal eSafety Incident  
For Headteachers, Senior Leaders and eSafety Coordinators





# Appendix E

## E-Safety Incident Log

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

# Appendix F



## Personal Information Promise

The Information Commissioner's Office launched a Personal Information Promise in January 2009. St Albert the Great School has signed up to this promise.

### **The personal information promise is:**

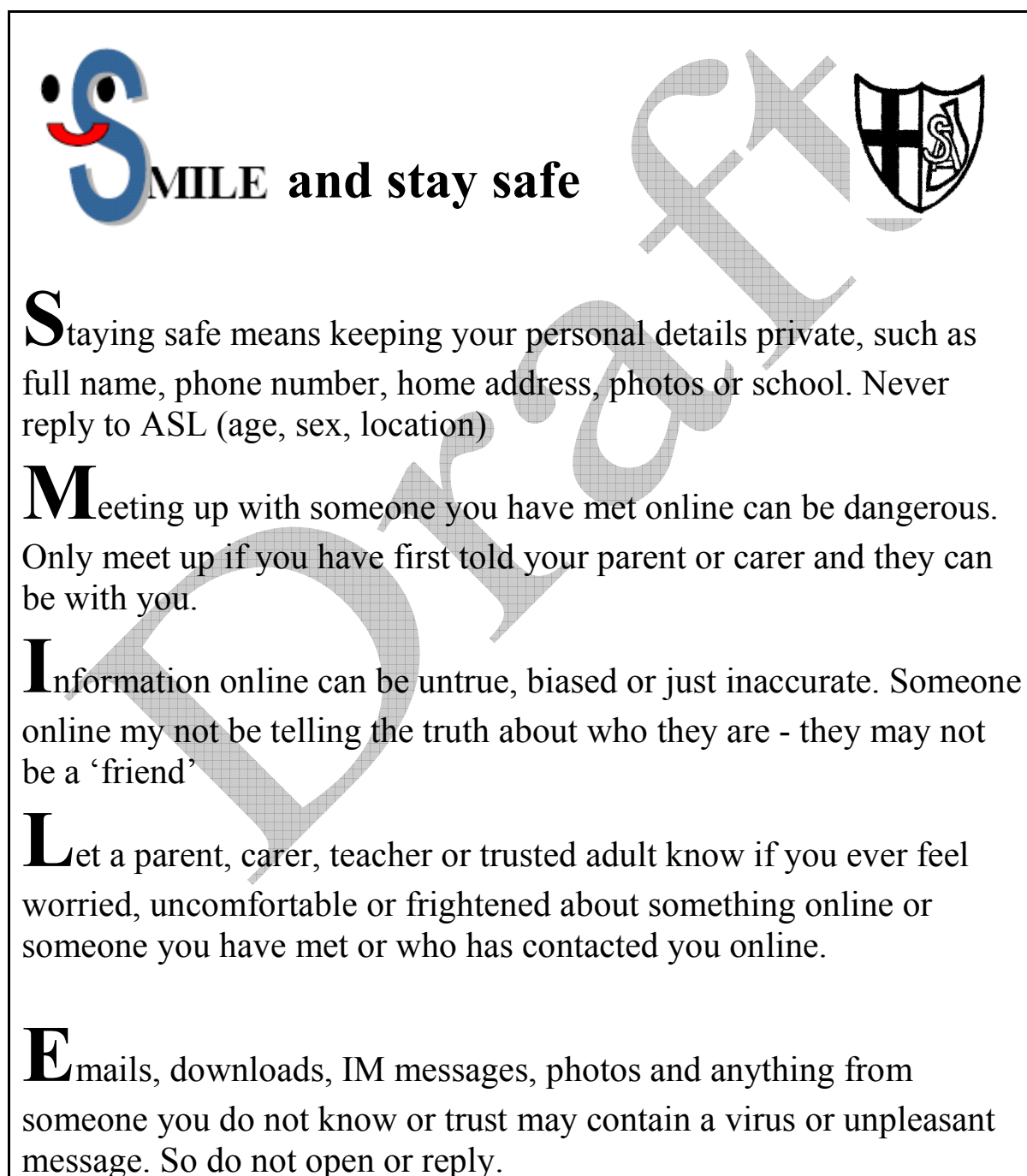
I, Louise Fleming, on behalf of St. Albert the Great Catholic Primary School, promise that we will:

1. value the personal information entrusted to us and make sure we respect that trust;
2. go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;
3. consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;
4. be open with individuals about how we use their information and who we give it to;
5. make it easy for individuals to access and correct their personal information;
6. keep personal information to the minimum necessary and delete it when we no longer need it;
7. have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;
8. provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly;
9. put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises; and
10. regularly check that we are living up to our promises and report on how we are doing

### **More information available -**

[http://www.ico.gov.uk/upload/documents/pressreleases/2009/personal\\_information\\_promise\\_280109.pdf](http://www.ico.gov.uk/upload/documents/pressreleases/2009/personal_information_promise_280109.pdf)

eSafety guidelines to be displayed throughout the school



The poster features a large, stylized blue letter 'S' with a smiling face (two black dots for eyes and a red curved line for a mouth). To the right of the 'S' is the text 'SMILE and stay safe' in a bold, black, sans-serif font. Further to the right is a black and white shield-shaped crest with a cross and a smaller emblem inside. The background of the poster is white with a faint, large, grey watermark of the word 'Smile' in a cursive font.

**S**taying 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)

**M**eeting 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.

**I**nformation online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a 'friend'

**L**et 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.

**E**mails, 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.



# Appendix H

## School e-Safety Policy in Brief

(This Policy in Brief should be issued to visitors, laminated and posted at workstations)



- At St. Albert the Great Catholic Primary School we have an e-safety policy which is reviewed at least annually, which all staff sign. Copies are kept on file. We use the LA model policy.
- ICT Acceptable Use Agreements are signed by all Staff/Governors/Students/Visitors. We use the 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.

Protected and Restricted material must be password protected if the material is to be removed from the school.

- We use SIMS to securely transfer CTF pupil data files to other schools.
- At St. Albert the Great Catholic Primary School we follow LA guidelines for the transfer of any other internal data transfer, using Outlook and SIMS.

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

- At St. Albert the Great Catholic Primary School we store such material in lockable filing cabinets in the school office.
- The school server is locked in the ICT suite and is managed by CRB-checked staff.
- We use follow LA back-up procedures and lock the tapes in a secure cupboard. Back-ups are encrypted and no back-up tapes leave the site.
- We use back up tapes for disaster recovery on our admin server.

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

- At St. Albert the Great Catholic Primary School we use the Authority's recommended current disposal firm for disposal of system hard drives where any protected or restricted data has been held.
- Paper based sensitive information is shredded..
- St. Albert the Great Catholic Primary School we are using secure file deletion software when school laptops are decommissioned.
- Laptops used by staff at home are brought in and disposed of through the same procedure
- SuperUsers with access to setting-up usernames and passwords which enable users to access data systems e.g. for email, network access, SLG and Learning Platform access are controlled by the LA and supported by Con-Ed Ltd.
- Security policies are reviewed and staff updated at least annually and staff know who to report any incidents where data protection may have been compromised. Staff have guidance documentation.

## Protective Marking Scheme: Information Assets: Risk Assessment Information

Senior Information Risk Owner  
(SIRO):

(named person)

(delete and change as appropriate)

Data and information assets	Impact Level (IL)	Data label	Information Asset Owner	Who has access to enter information	Purpose
ContactPoint	IL3	Restricted		Head / SENCO	ECM/statutory returns
<b>Pupil data (MIS)</b>					
Core pupil data	IL2	Protect		Senior Admin Officer/office administrators	ECM/statutory returns
Attendance	IL2	Protect		Senior Admin Officer/office administrators / class teachers	ECM/statutory returns
SEN	IL2	Protect		SENCO/ Senior Admin Officer	ECM/statutory returns
EAL	IL2	Protect		EAL Lead	ECM/statutory returns
Exclusion, behaviour	IL2	Protect		SENCO/ Senior Admin Officer/ class teachers / Deputy	ECM/statutory returns
Reports and assessments	IL2	Protect		Class teachers / Pastoral tutor / Headteacher	ECM/statutory returns
Tagged (named) student photos	IL2	Protect		Senior Admin Officer/office administrators	Safety/security
Unique Pupil Number (UPN)	IL3	Restricted		Senior Admin Officer/office administrators	ECM/statutory returns
Child protection data	IL3	Restricted			ECM/statutory returns
<b>Staff data (MIS)</b>					
Core staff data sets	IL2	Protect		Senior Admin Officer/Bursar	ECM/statutory returns
Training and absence data	IL2	Protect		Senior Admin Officer/Bursar / Deputy headteacher	ECM/statutory returns
<b>Finance system</b>					
Purchase Orders, Invoices, Payments	IL2	Protect		Senior Admin Officer/Bursar	Sound financial management
Approvals and budget setting	IL2	Protect		Head	Sound financial management
<b>Access control / passwords</b>					
Network password lists	IL2	Protect		Network Manager	Access to system(s)
Learning Platform password information	IL2	Protect		School LMLE SuperUser administrator	Access to system(s)
Learning Platform password information	IL2	Protect		LP administrator	Access to system(s)
<b>Disaster recovery contact system</b>					
Parental messaging system information	IL2	Protect		Senior Admin Officer/ Head / Deputy	Business continuity/communication
Emergency mobile phone loaded with data	IL2	Protect		Head / Deputy / Senior Admin Officer	Business continuity/communication

Other potentially sensitive material					
Tagged (named) student photos	IL2	Protect		Class teachers / Network Manager	Teaching and learning
Learning Platform	IL2	Protect		Class teachers / LP SuperUsers	Teaching and learning
School website	IL2	Protect		Office administrator / web officer / Head	Business continuity/communication
Information sent to parents	IL1	Unclassified		Head / Deputy / Class teachers	Business continuity/communication
<i>schools' other systems - specify</i>					

Last updated:

Updated by:

This should be regarded as work in progress and will be amended following national / regional advice (could [include Risk Assessment information](#) if desired – see

Draft