eSafety and Data Security Policy

Person responsible: Headteacher

This version: May 2015

Review Date: May 2017

Contents

Introduction	3
Senior Information Risk Owner	4
Information Asset Owner	4
Monitoring	5
Breaches	5
Incident Reporting	5
Computer Viruses	5
Data Security	5
Security	6
Impact Levels and Protective Marking	6
Disposal of Redundant ICT Equipment Policy	7
e-Mail	8
Equal Opportunities	11
eSafety	11
Internet Access	12
Parental Involvement	13
Passwords and Password Security	14
Personal, Sensitive, Confidential and Classified Information	15
Safe Use of Images	15
School ICT Equipment	17
Servers and backups	19
Systems and Access	19
Appendix 1- Pupil Acceptable Use Agreement/eSafety Rules	**22**
Appendix 2 - Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct	**23**

Alban City School
eSafety and Data Security Policy

1. Introduction

Information and Communications Technology (ICT) in the 21st Century is an essential resource to support learning and teaching, and plays 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.

ICT 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.
- Learning Platforms and Virtual Learning Environments.
- E-mail and Instant Messaging.
- Chat Rooms and Social Networking.
- Blogs and Wikis.
- Podcasting.
- Video Broadcasting.
- Music Downloading.
- Gaming.
- Mobile/ Smart phones with text, video and/ or web functionality.
- Other mobile devices with web functionality.

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Alban City 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.

Schools hold personal data on learners, staff and other people 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 the school to use technology to benefit learners.

Everybody in the 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 should be made aware of the risks and threats and how to

minimise them.

We recognise that the users to which this policy applies cover Staff, Governors, consultants/ contractors working at the school, Parents and Pupils of Alban City School. The issues for each of these user groups are slightly different and as such this policy and the Acceptable Use Agreement will apply to all users unless stated otherwise. The policy and Acceptable Use Agreement apply to all ICT equipment, whether supplied by the school or technologies owned by pupils, staff and governors brought onto school premises. ICT equipment is inclusive of both fixed and mobile Internet; PCs, laptops, Smartphones, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, portable media players, etc). The policy also applies to any school related data wherever it is stored-on-site or off-site.

2. Roles and responsibilities

a) Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff who is familiar with information risks and the school's response. At Alban City School the SIRO is the headteacher who has the following responsibilities:

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

The SIRO is supported in this role by *Managing Information Risk*, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] produced by the office of Public Sector Information.

b) Information Asset Owner (IAO)

The role of an IAO is to understand:

- What information is held and where it is held (e.g. in the MIS, on paper), for what purposes, whether or not it is sensitive.
- 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 of.

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

At Alban City School the information asset owner is the business manager.

c) e-safety co-ordinator

The named eSafety co-ordinator in this school is the Headteacher who has been designated this role as a member of the senior leadership team. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Herts LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet. All members of the school community must be made aware of who holds this post.

d) Staff, Governors, Consultants, Parents and Pupils

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.

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 PSHE.

3. Monitoring

All Internet activity is logged by the school's Internet provider, Herts for Learning. These logs may be monitored by their authorised staff, and the school will be contacted if any inappropriate activity is detected. In addition, the head or business manager may review these logs from time to time.

4. Breaches

A breach or suspected breach of policy by a School employee, governor, 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

Policy breaches may also lead to criminal or civil proceedings.

5. Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's SIRO. 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 schools SIRO.

6. Computer Viruses

All files downloaded from the Internet, received via e-mail or on removable media (e.g. USB drive) must be checked for any viruses using school provided anti-virus software before using them.

Under no circumstances may any staff, governors, pupils or parents interfere with any anti-virus software installed on school ICT equipment. Anti-virus software is

regularly updated by the ICT support provider, Herts for Learning.

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

7. Data Security

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

The school follows 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.

8. Security

- The School gives relevant staff access to its Management Information System, with a unique ID and password. Staff should not share these passwords with other staff and if they are compromised or shared by mistake they should be changed immediately.
- Staff are issued with the relevant guidance documents and the Policy for ICT Acceptable Use and are made aware of their responsibilities when accessing school data when they join the school.
- Staff must 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/).
- Staff must keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
- Staff must 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 must 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.
- Confidential information should not be sent by fax unless with the express

permission of the headteacher. The use of the HCC secure platform for safeguarding should be used where possible for transfer of confidential information.

9. Impact Levels and Protective Marking

The SIRO will provide guidance on how to label data to help reduce the risk of security incidents. Applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of an organisation's business. Applying too low a protective marking may lead to damaging consequences and compromise of the asset.

At Alban City school the labelling classifications used are as follows:

- PROTECT e.g. personal information about an individual- pupil, staff, parents, governors.
- RESTRICTED- Information that should not be shared outside of the two people that are discussing or sharing it.
- UNCLASSIFIED – All other documents.

All files, either digital or paper, should be marked with one of these classifications unless they are public information. The sensitivity of an asset may change over time and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within its contents.

10. Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorized agency or via the Hertfordshire Business Services (HBS) disposal scheme. 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 authorized 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

http://www.ico.gov.uk/what_we_cover/data_protection.aspx

Electricity at Work Regulations 1989

http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- The business manager 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
    - Authorization for disposal, including:
        - verification of software licensing
        - any personal data likely to be held on the storage media
    - How it was disposed of e.g. waste, gift, sale
    - Name of person & / or organisation who received the disposed item

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.

11. e-Mail

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. E-mails sent on school equipment may be accessed and read by the school if appropriate. 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 good network etiquette; 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving e-mails.

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 as all emails are stored. The user email account provided by the school should be the account that is used for all school business. The e-mail policy applies however e-mail is accessed (whether directly, through webmail when away from the office or on non-school hardware).

Staff

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
- Under no circumstances should staff contact pupils, parents or conduct any

school business using personal e-mail addresses.

- The use of Hotmail, BTInternet, AOL or any other third-party webmail service, other than the officially supported Microsoft Office 365 Education webmail platform for sending, reading or receiving business related e-mail is not permitted.

- 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' etc. This has been set up for all account holders by Herts for Learning.

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

- Staff must use their own school e-mail account so that the originator of a message is easily identifiable.

- All e-mails sent by staff are subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Staff must therefore actively manage your e-mail account as follows:

    - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives.
    - E-mailing parents directly is discouraged, but all correspondence with parents should be kept for a period of 3 years before being deleted.
    -

- Staff must inform the headteacher if they receive an offensive e-mail.

- If sending e-mails containing data classified as PROTECT or RESTRICTED to external third parties or agencies, refer to the Section 12.4.

- Staff should not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.

- Staff should keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.

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

Pupils

- 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.

Governors

- Governors should never discuss school issues with parents or pupils by e-mail, unless acting as a Governor in the dialogue.

- Governors should only use e-mail correspondence with each other and school staff to discuss the business of the governing body and should take care never to disclose personal or confidential information by e-mail.

- Governors are permitted to use personal e-mail accounts for school business.

12.2 General e-mail advice

- Users should always log out of your account when finished.

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

12.4 e-mailing Information classified as RESTRICED or PROTECT

- All such classified information must be transmitted through the office unless approved by the Headteacher.
- 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, and faxing sensitive or confidential information should also be avoided.

- 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.
    - Before releasing the e-mail:

        1. Verify the details, including accurate e-mail address, of any intended recipient of the information.
        2. Verify (by phoning) the details of a requestor before responding to e-mail requests for information.
        3. 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 (See office staff for how to do this)
    - 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.

HCC provide a secure platform to transfer data to specific external agencies. Such arrangements are currently in place with:

- Hertfordshire Constabulary.
- Hertfordshire Partnership Trust.

13 Pupils with Additional Needs

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

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 and young people.

14 eSafety in the curriculum

ICT and online resources are increasingly used across the curriculum at Alban City School. eSafety is embedded within our curriculum and we continually look for new opportunities to promote it. For example:

- The school provides opportunities within a range of curriculum areas to teach about eSafety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the computing curriculum.
- Pupils are taught about respecting other people's information, images, etc. through discussion, modelling and activities.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the computing curriculum.
- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, and depending on the seriousness of the offence; investigation by the Headteacher/ Governors or immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

15. Internet Access

The Internet is an open communication medium, available to all, 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 use of the **Hertfordshire Grid for Learning** (HGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

15.1 Managing the Internet

- Pupils will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile Internet technology.
- Staff will preview any recommended sites before use.
- All image searches performed by pupils are to be supervised
- If Internet research is set for homework, specific sites will be suggested that have previously been checked where possible by the teacher. It is advised that parents check 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.

15.2 Internet Use

- Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.
- Users must not reveal names of colleagues, pupils, parents or governors or any other confidential information on any social networking site or blog.
- On-line gambling or gaming is not allowed.

Staff are permitted to use the Internet for work purposes at any time and for personal use only during a scheduled break. Pupils are only permitted to use the Internet under the supervision of school staff and during planned lessons.

15.3 Infrastructure

- 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
- Staff and pupils are aware that school based email and Internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.
- If there are any issues related to viruses or anti-virus software, the business

manager should be informed immediately.

16. Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school and also to be aware of their responsibilities. We aim to regularly discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website).
- The school disseminates information to parents relating to eSafety where appropriate in the form of;
    - Information and celebration evenings
    - Posters
    - Website/ Learning Platform postings
    - Newsletter items
    - Learning platform training.

17. Passwords and Password Security

17.1 Passwords

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security.
- Users must always use their own personal passwords to access computer based services.
- Users must enter their personal passwords each time they logon. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Staff are expected to have secure passwords which are not shared with anyone.
- Herts for Learning will initiate an annual password change for all staff every September.
- Pupils are expected to keep their passwords secret and not to share with others, particularly their friends.
- Passwords should be at least 12 characters long and contain a mixture of at least 3 types of uppercase, lowercase, numbers and symbols
- Passwords must be changed whenever there is any indication of possible system or password compromise and this should be reported to the ICT support team.

- User accounts for staff and pupils who have left the School are removed from the system within a week of them leaving.

18. Personal, Sensitive, Confidential and Classified Information

18.1 Protecting Personal, Sensitive, Confidential and Classified Information

- Staff should not disclose any personal, sensitive or confidential information without prior permission from the head and must ensure the accuracy of any personal, sensitive, confidential and classified information disclosed.

- Staff and governors should 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.

- Only download personal data from systems if expressly authorised to do so by the headteacher.

- Staff and governors should keep their screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.

- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling.

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

- Staff should not use removable media for personal, sensitive or confidential information.

19 Safe Use of Images

19.1 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://connect.hertscc.gov.uk/connect/news/images/?view=connect

The school permits the appropriate taking of images by staff and pupils with school equipment with the written consent of parents (on behalf of pupils) and staff.

19.2 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 in the following ways:

- on the school web site.
- on the school's Learning Platform.
- in the school prospectus and other printed publications that the school may produce for promotional purposes.
- 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/ 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 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.

Teachers and office staff 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.

19.3 Storage of Images

- Images/ films of children are stored on the school's network.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform.

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

20.1 School ICT Equipment

- All users of school ICT are responsible for any activity undertaken on the

school's ICT equipment provided to them.

- Alban City School logs ICT equipment issued to staff and records serial numbers as part of the school's inventory.

- Users must 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.

- Users must save data on a frequent basis to the school's network drive to ensure that it is backed up regularly. Users are responsible for the backup and restoration of any data that is not held on the school's network drive.

- Personal or sensitive data should not be stored on the local storage of ICT equipment. If it is necessary to do so the local storage must be encrypted.

- It is recommended that a time locking screensaver is applied to all machines. Any PCs etc. accessing personal data must have a locking screensaver as must any user profiles.

- Staff must return all ICT equipment to the Headteacher on termination of employment, resignation or transfer, and provide details of all their user accounts so that they can be disabled.

20.2 Portable & Mobile ICT Equipment

This section covers such items as laptops, PDAs 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 school's 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.

- 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 headteacher, fully licensed and only carried out by your ICT support.

20.3 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. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to

children outside of school too. 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.

20.4 Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members 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.

21. Servers and backups

- Servers will be encrypted, therefore password protecting data.
- Access rights to servers will be implemented in such a way as to ensure only authorised users can gain access to PROTECT or RESTRICTED information.
- All backup tapes are encrypted.
- Data must be backed up daily onto tapes. There are 5 Friday tapes, 3 termly tapes and 1 annual tape so that data for the past year is kept.
- Back-up tapes must be securely stored in the office fireproof safe.
- One termly tape will be stored off site in a secure location (currently locked box at Business Managers home).
- Remote back-ups should be automatically securely encrypted. Herts for Learning provide an encrypted remote back up service, which Alban City School uses to back up office data (but not curriculum data).

22. Other rules for all users of ICT in school

- Users must not introduce or propagate viruses.
- Users must 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 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, permission must be obtained from the owner or owning authority and any relevant fees paid before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.

- It is essential that any storage devices which may have held personal or confidential data are securely erased, this can be arranged through the school business manager.

- Alban City School has engaged Herts for Learning to manage the school's IT support. Their employees are subject to the following checks (as taken from Herts for Learning's employee handbook):

  If you are in a position which requires you to work in a school on a regular basis you must:

  a) have a DBS enhanced check (with a children's barred list check), ***and***

  b) register with the DBS Update Service not later than 14 calendar days after the date of issue of the DBS certificate. The company will pay for the check and update service, but if you fail to register in time with the DBS update service the Company will be required to carry out a recheck, the cost of which may be deducted from your salary

  If you are in such a role you will be required to provide the Company with the original DBS disclosure certificate in order that a copy can be taken which will be kept on your personal record file and, in line with the requirements of the Update Service, you are required to keep your personal information accurate and up to date on an ongoing basis.

  If you are not in a role which requires you to work in a school on a regular basis the company will carry out a 'Basic' check only. Employee Handbook Updated: June 2014 Page 15 of 18

Appendix 1 - Pupil Acceptable Use Agreement/eSafety Rules

Dear Parent/ Carer

ICT including the Internet, e-mail and mobile technologies, etc 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 do not sign and return this form your child will not be able to use the Internet in school.

- 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 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.
- I will not take and use any photos, videos or voice recordings of someone else without their consent.

We have discussed this and …….....(child's name) agrees to follow the eSafety rules and to support the safe use of ICT at Alban City School.

Parent/ Carer Signature ……..……

Class …… Date ……

Appendix 2 - Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

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 agreement 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 agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with The Headteacher.

- I have read the school's eSafety and Data Security policy and I will comply with it.
- I will support and promote the school's eSafety and Data Security policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature

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

Signature …….…… Date ……

Full Name …….....(printed)

Position . . . . . .