Great Wilbraham School E-Safety Policy (rev.1.1 July, 2015)

Contents

Appendices:

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Great Wilbraham Primary School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Great Wilbraham primary school.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyber-bullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Children to understand criminal age of responsibility.
- Understand the risk of grooming and how and what this is with real life experiences.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.
- Have a clear mechanism of referral of incidents and recording of e-safety concerns and issues (use concern forms)
- Access to illegal, harmful or inappropriate images.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites.
- Content validation: how to check authenticity and accuracy of online content (understanding age verification laws and criminal age of responsibility).

Contact

- Grooming.
- Cyber-bullying in all forms.
- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords.

Conduct

- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well-being (amount of time spent online (internet or gaming).
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images).
- Copyright (little care or consideration for intellectual property and ownership – such as music and film).

(Ref Ofsted 2013)

Scope

This policy applies to all members of Great Wilbraham community (including staff, students / pupils, governors, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of Great Wilbraham Primary School.

The Education and Inspections Act 2006 empowers Head teacher's to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The *school* will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-Safety provision. • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements (Cambridgeshire County Council & DfE). • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant. • To be aware of procedures to be followed in the event of a serious e-Safety incident. • Use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation. • To receive regular monitoring reports from the E-Safety Co-ordinator re; events, outside organisations and specific training tools.

Role	Key Responsibilities

E-Safety Co-ordinator / Designated Child Protection Lead	• Takes day to day responsibility for e-safety issues and has a leading role in establishing, writing and reviewing the school e-safety policies / documents.
	• Promotes an awareness and commitment to e-safeguarding throughout the school community.
	• Ensures that e-safety education is embedded across the curriculum and linked to ICT and PSHCE.
	• Liaises with school ICT technical staff.
	• To communicate regularly with the designated e-Safety Governor to discuss current issues and review incident logs.
	• To ensure children are aware it is a positive resource to gain help and advice.
	• To ensure that all staff are fully aware of the procedures that need to be followed in the event of an e-Safety incident.
	• To ensure that an e-Safety incident log is kept up to date.
	• Facilitates training and advice for all staff.
	• Liaises with the Local Authority and relevant agencies.
	• Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • Sharing of personal data.
	  • Access to illegal / inappropriate materials.
	  • Inappropriate on-line contact with adults / strangers.
	  • Potential or actual incidents of grooming.
	  • Cyber-bullying and use of social media.

Governors / E-safety governor	• To ensure that the school follows all current e-Safety advice to keep the children and staff safe. • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Head Teacher receiving regular information about e-safety incidents and monitoring reports. A Brendan Reid , vice Chair of the Governing Body has taken on the role of E-Safety Governor. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include: • Regular review with the E-Safety Co-ordinator (including e-safety incident logs and training).
Computing Curriculum Leader	• To oversee the delivery of the e-safety element of the Computing curriculum. • To liaise with the e-safety coordinator regularly.
Network Manager/ Technician/	• To report any e-Safety related issues that arises, to the e-Safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date. • To ensure the security of the school ICT system.

Role	Key Responsibilities
	• To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices. • The school's policy on web filtering is applied and updated on a regular basis. • That he / she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant. • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures.
School Business Manager	• To ensure that all data held on pupils is adequately protected. • To ensure that all data held on pupils on the school office machines have appropriate access controls in place.
LA Nominated contact(s)	• To ensure all LA services are managed on behalf of the school including maintaining the database of access accounts and technical support.
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities. • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant). • To ensure that pupils are fully aware of how to and who to report any form of abuse or concern. • The professional and appropriate use of social media (e.g. don't encourage children to use twitter for a school project as brakes age verification laws).
All staff	• To read, understand and help promote the school's e-Safety policies and guidance. • To read, understand, sign and adhere to the school staff Acceptable Use Policy. • To be aware of e-safety issues related to the use of mobile phones, tablets, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices. • To report any suspected misuse or problem to the e-Safety coordinator. • To maintain an awareness of current e-Safety issues and guidance e.g. through CPD. • To model safe, responsible and professional behaviours in their own use of technology. • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Role	Key Responsibilities
Pupils	To understand the importance of reporting abuse, misuse or access to inappropriate materials. • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school. • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home. • To help the school in the creation/ review of e-safety policies. • Learn the value of password protection.
Parents/carers	• To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images. • To consult with the school if they have any concerns about their children's use of technology. • To attend or have details from E-safety evening.
External groups	• Any external individual / trainees/ organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school.

Communication:

How the policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted in the staffroom a mission statement on the website.
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school.
- Acceptable use agreements to be held in e-safety and/or personnel files.

Handling complaints:

- The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - Interview/counselling / e-Safety Coordinator / Headteacher.
  - Informing parents or carers.
  - Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system].
  - Referral to LA / Police / NSPCC.
  - Contact Cambridgeshire Constabulary 0845 456 4564, Education Child Protection Service Helpline 01223 712096, NSPCC Helpline 0808 800 5000.

- Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring

The e-safety policy is linked within other school policies: ICT and Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy and Personal, Social and Health Education.

- The school has an e-safety coordinator who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies or legislation in use within the school or wider community

- The e-safety policy has been written by the school e-safety Coordinator, Mr Paul Cherry and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy. All amendments to the school e-Safeguarding policy will be discussed in detail with all members of teaching staff.

Version Control

As part of the maintenance involved with ensuring your e-safety policy is updated, revisions will be made to the document. It is important that the document owner ensures the document contains the following information and that all revisions are stored centrally for audit purposes.

Title	Great Wilbraham e-safety policy
Version	1.1
Date	21/06/2015
Author	e-safety coordinator (Paul Cherry)
Approved by Headteacher	July 2015 Mrs Etchie
Approved by Governing Body	July 2015
Next Review Date	July 2017

2. Education and Curriculum

Pupil e-Safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHCE curriculum. It is built on LA / e-Safeguarding and e-literacy framewok for EYFS to Y6/ national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the

internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine/NSPCC or the CLICK CEOP button.

- To STOP and THINK before they CLICK.
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be.
- To know how to narrow down or refine a search.
- To understand how search engines work and to understand that this affects the results they see at the top of the listings.
- To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- To understand why they must not post pictures or videos of others without their permission.
- To know not to download any files – such as music files - without permission.
- To have strategies for dealing with receipt of inappropriate materials.
- To understand why and how some people will 'groom' young people for sexual reasons.
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include risks in pop-ups; buying on-line; on-line gaming / gambling.

- Children know age of criminal responsibility.

Staff and governor training

This school:

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues and the school's e-safety education program; annual updates, staff meeting, NSPCC on-line training.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-Safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

This school:

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear.
    - School newsletters; on the school web site.
    - Demonstrations, practical sessions held at school.
    - Suggestions for safe Internet use at home.
    - Provision of information about national support sites for parents.
    - Provide links to additional support agencies on school website.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- Are responsible for using the school ICT systems in accordance with the relevant policy.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
- To know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

Staff

- Are responsible for reading and agreeing the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students/Pupils

- Should have a good understanding of research skills and the need to uphold copyright regulations.

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school.
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident Management

In this school:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- Support is actively sought from other agencies as needed (e.g. CEOP, NSPCC, LA) in dealing with e-safety issues.
- Monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's Headteacher, Senior leaders and Governors.
- Parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

4. Managing the ICT infrastructure

- **Internet access, security (virus protection) and filtering**

This school:

- Has the educational filtered secure broadband connectivity through the LA and so connects to the 'private' National Education Network.
- Uses filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students.
- Uses DfE or LA approved systems, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site.
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform.
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons.
- Uses security time-outs on Internet access where practicable / useful.
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns.
- Ensures pupils only publish within an appropriately secure environment.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search , …..
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search.
- Informs all users that Internet use is monitored.
- Informs staff and students that that they must report any failure of the filtering systems directly to the [system administrator / teacher). Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LA Helpdesk as necessary.

- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme.
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents.
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

- **Network management (user access, backup)**

  This school:
  - Uses individual, audited log-ins for all users.
  - Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
  - Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful.
  - Ensures the Systems Administrator / network manager is up-to-date with Cambs services and policies / requires the Technical Support Provider to be up-to-date with Cambs services and policies.
  - Storage of all data within the school will conform to the UK data protection requirements.

    Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also provide a different username and password for access to our school's network.
- We provide pupils with a log-in. We are working towards when they are also expected to use a personal password; which will result in all pupils having their own unique username and password which gives them access to the Internet.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network.
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- Requires all users to always log off when they have finished working or are leaving the computer unattended.

- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves. Users needing access to secure data are timed out after and have to re-enter their username and password to re-enter the network.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed.
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with agreed policies.
- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved suppliers / LA electrical engineers.
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems e.g. teachers access their area / a staff shared area for planning documention.
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child.
- Makes clear responsibilities for the daily back up of finance systems and other important files.
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA.
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use.
- All computer equipment is installed professionally and meets health and safety standards.
- Projectors are maintained so that the quality of presentation remains high.
- Reviews the school ICT systems regularly with regard to health and safety and security.

Passwords policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use passwords to access SIMS and log on.
- It is suggested staff change their passwords on an annual basis.

E-mail

This school:

- Provides staff with an email account for their professional use, SIMS (Cambridgeshire Education Portal) email and makes clear personal email should be through a separate account.
- Does not publish personal e-mail addresses of pupils or staff on the school website.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date.
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use various technologies to help protect users and systems in the school, including desktop anti-virus to help detect Trojans, pornography, phishing and inappropriate language.

Pupils:

- Pupils are introduced to e-mail as part of the ICT/Computing scheme of work.
- Pupils are taught about the safety and 'etiquette' of using e-mail both in school and at home i.e. they are taught:
    - Not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer.
    - That an e-mail is a form of publishing where the message should be clear, short and concise.
    - That any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
    - They must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.
    - To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe.

- That they should think carefully before sending any attachments.
- Embedding adverts is not allowed.
- That they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature.
- Not to respond to malicious or threatening messages.
- Not to delete malicious of threatening e-mails, but to keep them as evidence of bullying.
- Not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them.
- That forwarding 'chain' e-mail letters is not permitted.

Staff:

- Staff only use LA (unless specified different or in the event of a system failure or emergency) e-mail systems for professional purposes.
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems.
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school style i.e. correct font:
    - The sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used.
    - The sending of chain letters is not permitted.
    - Embedding adverts is not allowed.
- All staff signs our school Acceptance Use Policy (AUP) to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School website

- The senior leadership team takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- The school web site complies with the statutory DfE guidelines for publications.
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. office@schooladdress. Home information or individual e-mail identities will not be published.
- Photographs published on the web do not have full names attached.
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.
- We do not use embedded geo-data in respect of stored images.
- We expect teachers (in the future) using' school approved blogs to password protect them and run from the school website.

Learning platform/Staff share

- Uploading of information on the schools' staff share is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas.
- Photographs and videos uploaded to the schools staff share will only be accessible by members of the school community.

Social networking

- Teachers are advised not to run social network spaces for school, but to use the schools' preferred system for such communications.
- Take guidance from Childnet, NSPCC (Net Aware) & ChildLine. concerning social networking sites introduce e-safety evening and link to teaching practise within ICT and PSHCE curriculum.

School staff will ensure that in private use:

- No reference should be made in social media about students / pupils, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.

- Staff should adhere to the Safer code of Conduct policy (latest version)
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing (whole school)

- Only use the LA / or approved services for video conferencing activity.
- Only use approved or checked webcam sites.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Headteacher is the Senior Information Risk Officer (SIRO).
- We ensure staff know who to report any incidents where data protection may have been compromised. Report to Head Teacher, e-safety co-ordinator and/or report incidence on E-safety incident form (NSPCC) always kept in e-safety file in Head Teachers office.
- All staff are DBS checked and records are held in one central record.

  We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

  - Staff.
  - Governors.
  - Parents.

  This makes clear staffs' responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff and Governors to undertake annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have staff share to store sensitive documents or photographs.
- It is advised that staff log-out of systems when leaving their computer.
- We store any Protect and Restricted written material in appropriate storage cabinets.
- All servers are managed by DBS-checked staff.
- We comply with the WEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and obtain a certificate of secure deletion for any server that once contained personal date (or follow Cambs protocol).
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded using a cut shredder.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Staff members may use their phones during school break times or other times if in an event of any emergency or unique circumstances. All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices

- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone.
- No students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.

Digital images and video
In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs.
- All staff will sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use.
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Asset disposal

Details of all school-owned hardware and software will be recorded. All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Additional assistance & Guidance
NSPCC/ChildLine
Childnet
CEOP