SANDY UPPER SCHOOL

POLICY

E-SAFETY

Effective Date:

Last Reviewed:

Reviewed by:

Next Review Date:

Contents	Page No

Introduction

Information Communication Technology (ICT) in the 21st century is seen as an essential resource to support independent learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, Sandy Upper School needs to develop the use of these technologies in order to arm our students 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
- Email 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

Although ICT is exciting and beneficial both in and out of the context of education, we must recognise that some resources, 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.

Here at Sandy Upper School, we understand the responsibility to educate our students on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy and the Acceptable Use Agreement (for all Staff, Governors, Visitors and Students) are inclusive of both fixed and mobile internet; technologies provided by the School - PCs, laptops, personal digital assistants, tablets, whiteboards, digital video equipment, etc; and technologies owned by students and staff, but brought onto School premises - laptops, mobile phones, camera phones, PDAs and portable media players, etc.

Roles and Responsibilities

As E-Safety is an important aspect of strategic leadership within the School, the Principal and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. A member of the Senior Leadership Team has been designated the role as the E-Safety Co-ordinator. All members of the School community have been made aware of who holds this post. It is the role of the E-Safety Co-ordinator to keep abreast of current issues and guidance through organisations such as Central Bedfordshire Council, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Leadership and Governors are regularly updated by the Principal/E-Safety Co-ordinator and all Governors have an understanding with regard to the issues and strategies at our School in relation to local and national guidelines and advice.

This policy, supported by the School's acceptable use agreements for staff, Governors, visitors and students, is to protect the interests and safety of the whole School community. It is linked to the following mandatory School policies and other documents: Child Protection, Health and Safety, Home–School Agreements, and Behaviour/Student Discipline, including the Anti-Bullying Policy.

E-Safety Skills Development for Staff

- All staff will receive regular information and training on E-Safety issues in the form of In Service Training [INSET] and circulars.
- New staff will receive information on the School's acceptable use policy as part of an induction programme.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the School community (see attached flowchart.)
- All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas.

Managing the School E-Safety messages

- We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The E-Safety policy will be introduced to the students at the start of each School year.
- E-Safety posters will be prominently displayed.

E-Safety in the Curriculum

Students are introduced to E-Safety topics throughout various curriculums. A sample of E-Safety topics is shown below:

Year 9

The E-Safety unit introduces:

- Cyber bullying awareness.
- Use of the VLE.
- Research skills, website reliability and copyright.
- Risks to personal information.
- Social networking risks.

Year 10

The E-Safety unit introduces:

- Password security.
- Data security.
- Online shopping and security and website trustworthiness.
- Social networking safe and unsafe practices.
- Copyright and plagiarism.

Year 11

All students access an E-Safety programme that results in an externally accredited level 1 award in E-Safety. Topics assessed include:

- Potential risks associated with being online.
- How to protect yourself and your personal information online.
- How to behave responsibly and within the law.

KS4

The GCSE ICT course provides an opportunity for students to enhance their knowledge of:

- The use of usernames, passwords and other security measures.
- Control of access to and management of personal spaces.
- Threats to and methods of preventing misuse of personal information.
- The impact of relevant legislation.

More information about what is included in the ICT curriculum can also be found on the website under the Curriculum menu.

Safety advice and guidance

The School website has links to E-Safety advice for Parents/Guardians, Students and Staff as well as a link to CEOP (Child Protection and Online Protection) for further advice and guidance.

Password Security

- All users read and sign an Acceptable Use Agreement to demonstrate thatthey have understood the School's E-Safety Policy.

- Users are provided with an individual network and VLE log-in username. All students are expected to use a personal password and keep it private.

- Students are not allowed to deliberately access on-line materials or files on the School network, of their peers, teachers or others.

- If passwords have been compromised or someone else has become aware of your password, it must be reported to ICT technical support as soon as possible.

- Staff are aware of their individual responsibilities to protect the security and confidentiality of School networks, MIS systems and VLE, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

- Due consideration should be given when logging into the VLE to the browser/cache/cookie options (shared or private computer)

- At Sandy Upper School, all ICT password policies are the responsibility of ICT technical support and all staff and students are expected to comply with the policies at all times.

Data Protection

The accessing of School data is something that the School takes very seriously.

- Staff are made aware of their responsibility when accessing School data. They must not:
    - allow others to view the data
    - edit the personal data of a student held on the School Information Management System
    - remove sensitive or personal data from the School premises in electronic form unless the media is encrypted and transported safely
    - store data on an unsecured memory stick or the unencrypted hard drive of a laptop
    - retain personal or sensitive data for longer than required
    - send sensitive personal data via email unless it is from secure site to secure site

They must:

- ensure all personal information is securely destroyed (paper data to be shredded and hard drives are wiped using specialist software)
- ensure that where personal information is held on paper it is locked away when not in use or the office/desk is secure (i.e. locked when not occupied)

Other Relevant Policies

This policy should be read in conjunction with the School's Data Protection Policy.

Managing the Internet Safely

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 internet is logged and the logs are randomly, but regularly, monitored. Whenever any inappropriate use is detected it will be followed up.

- The School maintains that students 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.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents re-check these sites and supervise this work. Parents/guardians 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. Students will also reference any secondary or intellectual source within their work.

Infrastructure

- Staff and students are aware that School-based email and internet activity can be monitored and explored further if required.
- If staff or students discover an unsuitable site it must be reported to the ICT technical support as soon as possible.
- The School has an obligation to provide antivirus software and maintain up to date virus definitions for all managed devices.
- The School installs antivirus software on portable computers and the staff member to whom who it is assigned will have the responsibility of updating the virus definitions.
- The School installs an encryption drive (Deslock) on portable computers for staff members who have regular access to confidential data.
- Students and staff are not permitted to download programmes or files on School based technologies without seeking prior permission from ICT technical support

Managing other Web 2 Technologies

Web 2/Social networking sites, if used responsibly both outside and within an educational context, can provide easy to use, creative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the School endeavors to deny access to social networking sites to students.
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/home phone numbers, School details, email address, specific hobbies/interests).
- Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Students are encouraged to be wary about publishing specific and detailed private thoughts online.
- Students are asked to report any incidents of bullying to the School.
- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with students using the Sandy Upper Virtual Learning Environment [VLE] Platform or other systems approved by the Principal.
- Staff are prohibited from communicating or adding students still listed on role as “friends” on any social networking platform, instant messaging program or games service provider.
- Staff are prohibited from contacting students through personal emails and by text on their personal phones or on social media sites.

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.

Personal Mobile devices (including phones)

- The School allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the School allow a member of staff to contact a student or parent/guardian using their personal device.
- The School would prefer students not to bring personal mobile devices/phones to the School. If a student chooses to bring a mobile device to the School it must not be used for personal purposes within lesson time. At all times the device must be switched off.
- 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 the devices of any member of the School community.
- Users bringing personal devices into the School must ensure there is no inappropriate or illegal content on the device.

Mobile devices provided by the School (including phones)

- 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 the 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.
- Where the School provides a laptop for staff, only this device may be used to conduct School business outside of School.

Electronic Devices – Searching & Deletion

Part 2 of the Education Act 2011 (Discipline) sets out the powers afforded to Academies by statute to search students in order to maintain discipline and ensure safety.

The School has added power to search for items 'banned under the school rules' and the power to 'delete data' stored on electronic devices.

Items banned for personal use under the School rules are portable media devices, PDAs, gaming devices, mobile and smart phones.

Authorised persons can examine data on electronic devices if they think there is good reason for them to do so.

In determining 'good reason' to examine or erase the data or files, the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the School rules.

Responsibilities & Training

The Principal will authorise those staff that are allowed to carry out searches.

Members of staff authorised by the Principal to carry out searches for and of electronic devices, and to access and delete data/files from those devices, will receive training that is specific and relevant to this role.

In Carrying out a Search

The authorised member of staff carrying out the search must be the same gender as the student being searched; and there must be a witness (also a staff member) and they, too, should be of the same gender as the student being searched.

There is a limited exception to this rule. Authorised staff can carry out a search of a student of the opposite gender without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the Search

The person conducting the search may not require the student to remove any clothing, other than outer clothing.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets, but not an intimate search going further than that, which only a person with more extensive powers (e.g. a Police Officer) can do.

Use of force cannot be used to search without consent for items banned under the School rules regardless of whether the rules say an item can be searched for.

Where Inappropriate Material is Found

If inappropriate material is found on the device it is up to the authorised member of staff to discuss with the Principal whether they should delete that material, retain it as evidence (of a criminal offence or a breach of School discipline) or whether the material is of such seriousness that it requires the involvement of the Police.

Examples of illegal activity would include:

- Child sexual abuse images (including images of one child held by another child)
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

Recording, monitoring and reviewing

A record will be kept by the School of the reasons for the deletion of data/files.

The policy will be reviewed by the Principal and Governors annually and in response to changes in guidance.

Other Relevant Policies

This policy should be read in conjunction with the School's Behaviour Policy and the Anti-Bullying Policy.

Managing Email

The use of email within most Schools is an essential means of communication for both staff and students. In the context of the School, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between Schools on different projects, be they staff based or student based, within the School or international. We recognise that students need to understand how to style an email in relation to their age and good network etiquette (netiquette).

- The School gives all staff their own email account to use for all School business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

- 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, email histories can be traced. This is the account that should be used for all School business.

- Under no circumstances should staff contact students, parents or conduct any School business using personal email addresses.

- The School requires a standard disclaimer to be attached to all email correspondence, stating that:

"*This message contains information that may be privileged or confidential. It is intended only for whom it is addressed. If you are not the intended recipient, you are not authorised to read, print, retain, copy, disseminate, distribute or use this message or any part thereof. If you receive this message in error please notify the sender immediately and delete all copies of this message.*

As Internet communications are not secure, please be aware that Sandy Upper cannot accept responsibility for its contents. It is, therefore, your responsibility to scan attachments (if any) for viruses. Any views or opinions presented are those of the author only and not of Sandy Upper School. Sandy Upper School reserves the right to intercept incoming and outgoing email communications."

- Emails sent to an external organisation should be written carefully before sending, in the same way as a letter written on School headed paper.

- Staff sending emails to external organisations, parents/guardians or students are advised to cc. their Line Manager.

- Students may only use School approved accounts on the School system. The accounts are restricted and can only send and receive emails from email accounts within Sandy Upper School.

- Individual student email accounts are created upon entry to the School in Year 9.

- All email users are expected to adhere to the generally accepted rules of network etiquette, particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication.

- Students must immediately tell a teacher/trusted adult if they receive an offensive email.

- Staff must inform technical support if they receive an offensive e-mail or emails that can be considered as Spam.

Safe Use of Images

Sandy Upper School Safeguarding

Staff/Governors/Visitors

Guidelines for safe use of images of students please read carefully

Taking of Images and Film

- With the support of parents/guardians (on behalf of students) and Staff, Governors and Visitors, the School permits the appropriate taking of images by staff and students with School equipment.

- Staff/Governors/Visitors/Students are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, including when on field trips or enrichment days, without the express permission of the Principal. When permission has been given, images taken must then be transferred immediately and solely to the School's network and deleted from the portable device.

Publishing Students' Images and Work

Parents/Guardians will be asked to support the School in allowing images of their children to be recorded and displayed, including photographs, in the following ways:

- Sandy Upper School website, the Prospectus, Newsletter, plasma screens, curriculum documents and local press releases. The photographs used will show School Visits, Trips, Enrichment Days, student success/celebration, e.g. Year 11 Prom, celebration assemblies, sport team presentations, examination results day, charity events

- Displays within the School

- External exhibitions

This support is considered valid for the entire period that the child attends the School unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce, taken into care.

Storage of Images

- When permission has been given to Staff/Governors/Visitors or Students to use personal digital equipment, such as mobile phones and cameras, to record images of students, including when on field trips or enrichment days, images taken must then be transferred immediately and solely to the School's network and deleted from the portable device.
- Images/films of students are stored on the School's network only.
- Staff/Governors/Visitors and Students are not permitted to use portable media for storage of images e.g. USB sticks, without the express permission of the Principal.
- Rights of access to this material are restricted to the teaching staff and students within the confines of the School network.
- ICT technical support has the responsibility of deleting the images when they are no longer required, or the student has left the School.

CCTV and Webcams

- The School uses CCTV for security and safety. The only people with access to this are The Principal, IT Support Staff and Site Agents. Notification of CCTV use is displayed around the School.

- We do not use publicly accessible webcams in School.

Sandy Upper School Safeguarding

Staff/Governors/Visitors' Consent Form Please read carefully

Use of Photographs, Video or Web

As part of our Safeguarding Procedures we are attempting to make everyone connected with the School aware of our procedures regarding the use of photographs, video or web information related to them.

We use photographs or digital film in the School for a number of reasons. The main purpose is to celebrate success, achievement and any interesting or unusual events that take place – the photographs are used on display boards, on plasma screens, on the website, in *Sandy Spotlight* newsletter and occasionally in the local press or media.

We may also use film as a learning tool. For example, acting out scenes in Drama and then playing it back so that the teacher, the student and the class can analyse technique. Or, for example, in an interview situation, if this is relevant to a subject or piece of coursework. In most cases the film is only used within the School, but there may be cases where we use materials for public display and/or examinations.

Please note your name will normally be displayed alongside the photograph taken of you if it is of a small group or of an individual.

The Sandy Upper School therefore asks for your consent to using material, including photographs of you, in the following ways:

- Sandy Upper School website, the Prospectus, *Sandy Spotlight* newsletter, plasma screens, curriculum documents and local press releases. The photographs used will show School Visits, Trips, Enrichment Days, success/celebration e.g. Year 11 Prom, celebration assemblies, sport team presentations, examination results day, charity events

- Displays within the School

- External exhibitions/Press articles

If you need clarification or are concerned about the use of your photograph please contact Mrs M Walker, Principal's PA, at the School.

CONSENT FORM FOR COMPLETION BY STAFF/GOVERNORS/VISITORS

Please complete this section and return your signed Consent Form to Main Reception.

I **agree** to my photograph being used as described (please tick) ❒

I **do not agree** to my photograph being used as outlined (please tick) ❒

This Consent Form is considered valid for the entire period that you attend this School. You do have the right to withdraw consent at any time by writing to the Principal.

Staff/Governor/Visitor Name: ……..

Date: ……..

The Sandy Upper School

Safeguarding

Parental Consent Form – please read carefully

Use of Photographs, Video or Web

We use photographs or digital film in the School for a number of reasons. Themain purpose is to celebrate the success of students – the photos are used on displayboards, on the plasma screens, on the website and occasionally in the local pressor media. Examples include photographs of sports teams, members of the cast of School productions, extra-curricular activities, charity events and examinationsuccesses.

We may also use film as a Learning tool. For example, acting out scenes in Dramaand then playing it back so that the teacher, the student and the class can analysetechnique. In most cases the film is only used within the School, but there may be cases where we use materials for public display and/or GCSE moderation.

Please note your child's name will normally be displayed alongside the photograph if it is of a small group or just of your child.

The Sandy Upper School therefore asks for your consent to using material,including photographs, in the following ways:

- The Sandy Upper School website, the Prospectus, *Sandy Spotlight* newsletter, plasma screens, curriculum documents and local press releases. The photographsused will show School Visits, Trips, Enrichment Days, student success/celebration, e.g. Year 11 Prom, celebration assemblies, sport team presentations,examination results day, charity events

- Displays within the School

- External exhibitions/Press articles

If you need clarification or are concerned about the use of your child's photographplease contact Student Services at theSchool.

Students' photographs are also used on our Student Information Management System whichis only accessed by staff. They may also be used for emergency medical notes and bythe emergency services in exceptional circumstances.

This section to be completed by Parent/Guardian and returned to your child's Form Tutor

I **agree** to my child's photograph being used as outlined, please tick ☐

I **do not agree** to my child's photograph being used as outlined, please tick ☐

This Consent Form is considered valid for the entire period that your child attends this School unless there is a change in the child's circumstances where consent could be an issue.

Parents/Guardians do have the right to withdraw consent at any time by writing to the Principal.

Name of child_____ Form _____

Signe_____ (Parent/Guardian)

Date _____

If this form is not returned we reserve the right to assume that you give consent for your child to appear in any photographs as outlined.

Misuse and Infringements Complaints

Complaints relating to E-Safety should be made to the E-Safety Co-ordinator or Principal. Incidents should be logged and the flowcharts for managing an E- Safety incident should be followed.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the E-Safety Coordinator.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety Coordinator, depending on the seriousness of the offence; investigation by the Principal/LA, immediate suspension, possibly leading to dismissal and involvement of Police for very serious offences (see flowchart).

- Users are made aware of sanctions relating to the misuse or misconduct of IT equipment. Staff will all receive a full copy of the E-Safety policy and appropriate training and guidance. Governors, Parents, Students and visitors will all sign up to the User Acceptance Policy and where necessary, receive appropriate training and guidance.

Equal Opportunities

Students with Additional Needs

The School endeavours to create a consistent message with parents and guardians forall students and this in turn should aid establishment and future development of the School's E-Safety rules.

Staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues.

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

Parental Involvement

- Parents/Guardians 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, in *Sandy Spotlight* newsletter, on the Student Information Management System).

- The School disseminates information to parents/guardians relating to E-Safety where appropriate in the form of:

    - Website/ Learning Platform postings
    - Spotlight items
    - Guide for Parents
    - Awareness sessions on request

Acceptable Use Agreement: Staff, Governors and Visitors

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

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in the 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 E-Safety Coordinator, a member of the Senior Leadership Team.

- 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 Principal 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 students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to students.
- I will only use the approved, secure email system(s) for any School business.
- I will ensure that personal data (such as data held on SIMS) 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 the School or accessed remotely when authorised by the Principal or Governing Body.
- I will not install any hardware of software without permission of the E-Safety Coordinator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/ or staff will only be taken, stored and used for professional purposes in line with School policy and with written consent of the parent, guardian or staff member. Images will not be distributed outside the School network without the permission of the parent/guardian, member of staff or Principal.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Principal.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in the School and outside the School, will not bring my professional role into disrepute.
- I will support and promote the School's e-Safety policy and help students 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 use of ICT throughout the School.

This Consent Form is considered valid for the entire period I attend the School.

Signature: …….

Date: …….

Full Name (printed): …….

Job Title: …….

Dear Parent/Guardian

Use of the Internet by Students

In order to support Learning opportunities within the School your child will, at appropriate times, be given access to the Internet as an information source, a communications tool and a publishing medium.

The Internet has become a major source of educationally useful material and the primary distribution medium for a wide range of organisations. The potential to support the classroom teacher is significant and will continue to grow.

There are well-publicised concerns regarding access to material on the Internet that would be considered unsuitable for School students. Whilst it is impossible to ensure that a student will not access such material, the School is taking all reasonable steps to minimise a student's access to unsuitable material.

These include:

- Use of filtered Internet Service to prevent access to Internet sites with certain types of material e.g. pornography, violent, offensive and abusive material.
- Restricted access to 'chat rooms'
- The requirement that, wherever possible, all Internet access during School hours will be supervised by a member of staff or other responsible adult.
- Tracking mechanisms that enable the School to identify which Internet sites have been visited and to monitor Internet access.
- Educating students as to the potential legal consequences of accessing types of material.

Attached to this letter is a copy of the School's Acceptable Use Agreement. All users of the School equipment are expected to abide by this agreement. Users not abiding by this agreement may have their right to use the systems withdrawn. For serious offences, the Police or other authorities may have to be informed.

The School's policy on the use of computers and other technologies, including the use of the Internet is available for parents/guardians to inspect.

If you would like to discuss any issues surrounding the use of the Internet or the content of this letter please contact the School and ask to speak to me in the first instance.

Occasional awareness sessions regarding use of the Internet are run for parents and guardians, please ask for details.

Yours sincerely

E-Safety Coordinator

Acceptable Use Agreement: Students of Sandy Upper School

Student Acceptable Use Agreement / E-Safety Rules

- I will only use ICT systems in the School, including the internet, email, digital video, mobile technologies, etc. for School purposes.
- I will not download or install software on School technologies.
- I will only log on to the School network/ Learning Platform with my own user name and password.
- I will follow the School's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my School email address.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a School project approved by my teacher.
- Images of students and/or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the E-Safety Co-ordinator.
- I will ensure that my online activity, both in the School and outside the School, will not cause my School, the staff, students or others distress or bring into disrepute.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, School sanctions will be applied and my parent/guardian may be contacted.

Flowcharts for Managing an E-Safety Incident

Following an incident the E-Safety Coordinator and/or Principal will need to decide quickly if the incident involved any illegal activity

If you are not sure if the incident has any illegal aspects, contact Mrs Julie Devereux, Senior Child Protection Officer within Sandy Upper School on 01767 680598.

Was **illegal** material or activity found or suspected?

Yes

- Inform Police and the Sandy Upper School Technical Advisor. Follow any advice given by the police or otherwise.
- Confiscate any laptop or other device and if related to the School network, disable user account.
- Save ALL evidence but DO NOT view or copy. Let the Police review the evidence. If a student is involved, inform Mrs Julie Devereux, Senior Child Protection Officer within Sandy Upper School on 01767 680598.

No

Illegal means something against the law, such as:

- Downloading child pornography
- Passing onto others images or video containing child pornography
- Inciting racial or religious hatred

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to a member of staff or the E-Safety Coordinator

If the incident did not involve any illegal activity, follow the next flowchart relating to non-illegal activities

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

The E-Safety Coordinator and/or Principal should:

- Keep any evidence

Did the incident involve a member of staff?

Yes

If member of staff has:

1. Behaved in a way that has, or may have harmed a child
2. Possibly committed a criminal offence
3. Behaved towards a child in a way which indicates s/he is unsuitable to work with children

Contact Senior Child Protection Officer in school

- Review evidence and determine if the incident is accidental or deliberate
- Decide upon the appropriate course of action
- Follow School disciplinary procedures if deliberate

Incident could be:

- Using another persons username and password
- Downloading Adult pornography
- Accessing websites which are against School policy, eg, games
- Using a mobile phone to take a video during a lesson
- Using the technology to upset or bully (in extreme cases could be illegal)

No

Was the student the victim or instigator?

Student as victim

In-School action to support student by one or more of the following:

- Class Teacher
- E-safety Co-ordinator
- Senior Leader
- Principal
- Designated Senior Peron for Child Protection (DSP)

Inform parent/guardian as appropriate **if the child is at risk**.

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and talk to a member of staff or the E-Safety Coordinator

Student as instigator

Review incident and identify if other students were involved

Decide appropriate sanctions based on School rules/guidelines

Inform parents/guardians if serious or persistent incident

Review school procedures/policies to develop best practice

Sandy Upper School E-Safety Usage Report

Details of Internet usage/access to be recorded by ICT Technician. The reportwill be monitored periodically by the Principal or a member of theSLT.

Individual incidents are recorded and evidenced by the Intervention managers with the support of the ICT Technician.

Current Legislation

ACTS RELATING TO MONITORING OF STAFF EMAIL

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to School activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation. http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

OTHER ACTS RELATING TO E-SAFETY

Racial and Religious Hatred Act 2006

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

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust.

Communications Act 2003 (section 127)

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

The Computer Misuse Act 1990 (sections 1 – 3)

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

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

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

Malicious Communications Act 1988 (section 1)

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

Copyright, Design and Patents Act 1988

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

Public Order Act 1986 (sections 17 – 29)

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

Protection of Children Act 1978 (Section 1)

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

Obscene Publications Act 1959 and 1964

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

Protection from Harassment Act 1997

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

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

E-Safety Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for E-Safety policy. Staff that would contribute to the audit include: Designated Child Protection Coordinator, SENCO, E-Safety Coordinator, Network Manager and Principal.

Has the School an E-Safety Policy that complies with Central Bedfordshire LA and guidance	Yes
Date of latest update (at least annual):	
The School E-Safety policy was agreed by Governors on:	
The policy is available for staff at:	
The policy is available for parents/guardians at:	
The responsible member of the Leadership Team is:	
The Governor responsible for e-safety is:	
The Designated Child Protection Coordinator is:	
The E-Safety Coordinator is:	
Has E-Safety training been provided for both students and staff?	Yes
Is there a clear procedure for a response to an incident of concern?	Yes
Have E-safety materials from CEOP and Becta been obtained?	Yes
Do all staff sign a Code of Conduct for ICT?	Yes
Are all students aware of the School's E-Safety Rules?	Yes
Are E-Safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all students?	Yes
Do parents/guardians sign and return an agreement that their child will comply with the School E-Safety Rules?	Yes
Are staff, students, parents/guardians and visitors aware that network and Internet Use is closely monitored and individual usage can be traced?	Yes
Has an ICT security audit been initiated by the SIRO and IAO's?	Yes
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Yes
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements?	Yes
Has the School-level filtering been designated to reflect educational objectives and approved by SLT?	Yes
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SLT?	Yes
Have appropriate teaching and/or technical members of staff attended training on the Central Bedfordshire filtering system?	Yes

* Amended version to be presented to Governors'