E-Safety Policy Appendices

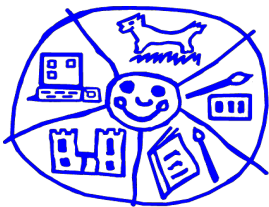Bungay Primary School

Appendices

1. Student Acceptable Use Policy Agreement
2. Staff and Volunteers Acceptable Use Agreement
3. Parent / Carer Acceptable Use Agreement
4. School Filtering Policy
5. School Password Security Policy
6. School Personal Data Handling Policy
7. Legislation
Glossary of terms

1. Student Acceptable Use Policy

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:
- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:
- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:
- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:
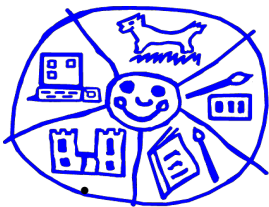
Bungay Primary School

- I will only use my personal hand held / external devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will only use chat and social networking sites with permission and at the times that are allowed
- When using the internet for research or recreation, I recognise that:
- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I understand that I am responsible for my actions, both in and out of school:
- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.
- Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

Student Acceptable Use Agreement Form
This form relates to the student Acceptable Use Policy (AUP), to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:
- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) e.g. mobile phones, PDAs, cameras etc.
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil_____ Form_____

Signed_____

Date_____

2. Staff and Volunteers Acceptable Use of IT Agreement

School Policy
New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:
- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students / pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

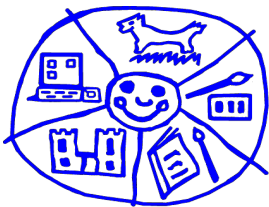**Acceptable Use Policy Agreement**
I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed eSafety in my work with young people.
For my professional and personal safety:
- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc.) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- When using the internet in my professional capacity or for school sanctioned personal use:
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff Name _____

Signed_____

Date_____
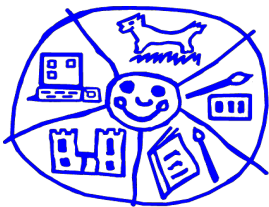
3. Parent/Carer Acceptable Use of IT Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:
- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of eSafety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carer Name_____

Student_____

- As the parent / carer of the above student(s), I give permission for my son / daughter to have access to the internet and to ICT systems at school.
- I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, eSafety education to help them understand the importance of safe use of ICT – both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's eSafety.

Signed_____ Date_____
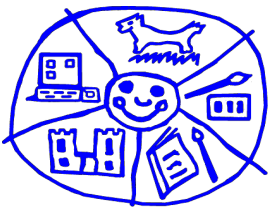
Use of Digital / Video Images

- The use of digital / video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons
- Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media
- The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.
- Parents are requested to sign the permission form below to allow the school to take and use images of their children.
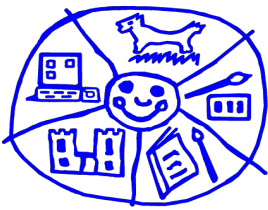
Permission Form

Parent / Carer Name_____
Student_____

As the parent / carer of the above student, I agree to the school taking and using digital / video images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed_____ Date_____

4. School Filtering Policy

Introduction
The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school. Bungay High School uses a self-managed filtering service, with some flexibility for changes at local level.

Responsibilities
The responsibility for the management of the school's filtering policy will be held by IT Services. They will manage the school filtering, in line with this policy and will keep records and logs of changes and of breaches of the filtering systems. To ensure that there is a system of checks and balances and to protect those responsible, changes to the filtering service must:
- be logged in change control logs
- be reported to the eSafety Governor every month in the form of an audit of the change control logs

All users have a responsibility to report immediately to IT Services any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered. Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / Training / Awareness
Students will be made aware of the importance of filtering systems through the eSafety education programme. They will also be warned of the consequences of attempting to subvert the filtering system. Staff users will be made aware of the filtering systems through:
- signing the AUP
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through eSafety awareness sessions / newsletter etc.

Changes to the Filtering System
Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to IT Services who will decide whether to make school level changes (as above).

Monitoring
No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School eSafety Policy and the Acceptable Use agreement. Monitoring will take place by using logs of filtering change controls and of filtering incidents, which will be made available to the eSafety Governor.

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.
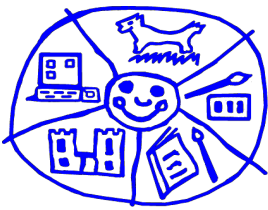
5. School Password Security Policy

Introduction

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies)
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure username / password system is essential if the above is to be established and will apply to all school ICT systems, including email and Virtual Learning Environment (VLE).

Responsibilities

- The management of the password security policy will be the responsibility of IT Services
- All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- Passwords for new users and replacement passwords for existing users can be allocated by IT Services. Any changes carried out must be notified to the manager of the password security policy (above)
- Users will change their passwords every 30 days. **Passwords must contain a combination of uppercase and lowercase letters and either number(s) or special character(s) (i.e. Norwich1 or Norwich@). First or last names cannot be used. The last five passwords are remembered."**

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's eSafety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in ICT and / or eSafety lessons (the school should describe how this will take place)
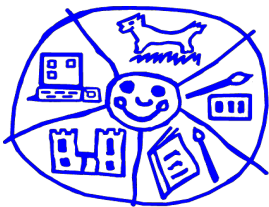- through the Acceptable Use Agreement

Policy Statements

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the eSafety Committee.

All users will be provided with a username and password by IT Services who will keep an up to date record of users and their usernames. Users will be required to change their password every term.

The following rules apply to the use of passwords

- passwords must be changed every term
- the last four passwords cannot be re-used
- the password should be a minimum of 6 characters long and
- the account should be "locked out" following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user

The "master / administrator" passwords for the school ICT system, used by IT Services must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe). (Alternatively, where the system allows more than one "master / administrator" log-on, the Headteacher or other nominated senior leader should be allocated those master / administrator rights. A school should never allow one user to have sole administrator access.

Audit / Monitoring / Reporting / Review
IT Services will ensure that full records are kept of:
- User IDs and requests for password changes
- User log-ons
- Security incidents related to this policy

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.
Local Authority Auditors also have the right of access to passwords for audit investigation purposes
User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

These records will be reviewed by eSafety Committee / eSafety Governor annually.

This policy will be regularly reviewed (preferably annually) in response to changes in guidance and evidence gained from the logs.

6. School Personal Data Handling Policy

Introduction
Schools should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature (Becta – Good Practice in information handling in schools – keeping data secure, safe and legal – Sept 2008).

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:
- have permission to access that data
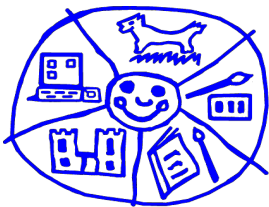- need to have access to that data.

Any loss of personal data can have serious effects for individuals the school, can bring the school into disrepute and may well result in disciplinary action and / or criminal prosecution. All transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data legislation and relevant regulations and guidance from the Local Authority.

The Data Protection Act (1998) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals (data subjects) with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow "good information handling principles".

Policy Statements
- The school will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.
- Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Fair Processing Code" and lawfully processed in accordance with the "Conditions for Processing".

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including students, members of staff and parents and carers e.g. names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members

Responsibilities

The School Business Manager will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs) for the various types of data being held (e.g. student information, staff information, assessment data etc.). The IAOs will manage and address risks to the information and will understand:

- what information is held and for what purpose
- how information has been amended or added to over time
- who has access to protected data and why

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents / Carers – the "Fair Processing Notice"

Under the "Fair Processing" requirements in the Data Protection Act, the school will inform parents / carers of all students of the data they hold on the students, the purposes for which the data is held and the third parties (e.g. LA, DCSF, Exam Boards, Connexions etc.) to whom it may be passed. This fair processing notice will be passed to parents / carers through the prospectus & newsletters, reports or a specific letter / communication. Parents / carers of young people who are new to the school will be provided with the fair processing notice.

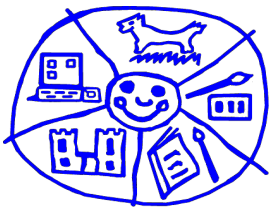A copy of a specimen fair processing notice can be found at: http://www.teachernet.gov.uk/management/ims/datamanagement/fpnpupils/. It contains a relevant wording for the regulations pertaining to the transfer of information to Connexions, in secondary schools and new requirements resulting from the introduction of ContactPoint.   A new specimen FPN is available for 2008/9. Schools are advised to contact their Local Authority for local versions of the Fair Processing Notice.

Training & Awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

Bungay Primary School

Identification of data

The school will ensure that all school staff, contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher.

All documents (manual or digital) that contain protected data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer:
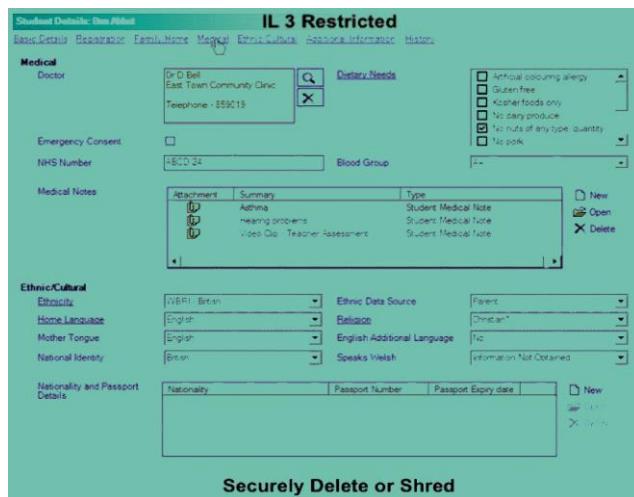

Impact levels are as follows:

- IL1–Not Protectively Marked (IL1–NPM)
- IL2–Protect
- IL3–Restricted
- IL4–Confidential

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data.

Release and destruction markings will be shown in the footer as follows:

[Release]	[Parties]	[Restrictions]	[Encrypt, Securely delete or shred]
The authority descriptor	The individuals or organisations the information may be released to	Descriptor tailored to the specific individual	How the document should be destroyed
Examples:			
Senior Information Risk Owner	School use only	No internet access No photos	Securely delete or shred
Teacher	Mother only	No information to father ASBO	Securely delete or shred
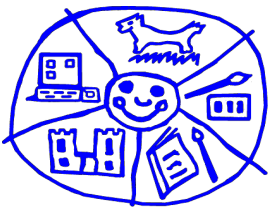
Secure Storage of and access to data

- The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.
- All users will be given secure user names and strong passwords which must be changed regularly. User names and passwords must never be shared.
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- Personal data can only be stored on school equipment (this includes computers and portable storage media). Private equipment (ie owned by the users) must not be used.

When personal data is stored on any portable computer system, USB stick or any other removable media:
- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

All paper based IL2-Protected and IL3-Restricted (or higher) material must be held in lockable storage. The school recognises that under Section 7 of the Data Protection Act, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests ie. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:
- Users may not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.
- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.
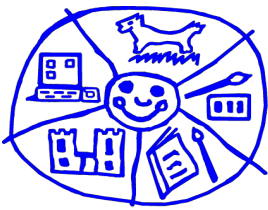
Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Audit Logging / Reporting / Incident Handling

- As required by the "Data Handling Procedures in Government" document, the activities of data users, in respect of electronically held personal information, will be logged and these logs will be monitored by the eSafety governor.
- The audit logs will be kept to provide evidence of accidental or deliberate security breaches – including loss of protected data or breaches of an acceptable use policy, for example. Specific security events should be archived and retained at evidential quality for seven years.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident
- a communications plan, including escalation procedures
- and results in a plan of action for rapid resolution and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Further reading

Teachernet – Data processing and sharing -
http://www.teachernet.gov.uk/management/atoz/d/dataprocessing/
Office of the Information Commissioner website: http://www.informationcommissioner.gov.uk
Office of the Information Commissioner – guidance notes: Access to student's information held by schools in England
Becta – Good Practice in information handling in schools – keeping data secure, safe and legal and its four detailed appendices: (September 2008) http://schools.becta.org.uk/upload-dir/downloads/information_handling.pdf
http://schools.becta.org.uk/upload-dir/downloads/information_handling_impact_levels.pdf
http://schools.becta.org.uk/upload-dir/downloads/data_encryption.pdf
http://schools.becta.org.uk/upload-dir/downloads/audit_logging.pdf
http://schools.becta.org.uk/upload-dir/downloads/remote_access.pdf
Cabinet Office – Datahanding procedures in Government – a final report (June 2008)
http://www.cabinetoffice.gov.uk/reports/data_handling.aspx

7. Legislation

Schools should be aware of the legislative framework under which this eSafety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority
- Obtain unauthorised access to a computer
- "Eavesdrop" on a computer
- Make unauthorised use of computer time or facilities
- Maliciously corrupt or erase data or programs
- Deny access to authorised users
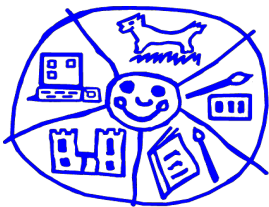
Bungay Primary School

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:
•   Fairly and lawfully processed
•   Processed for limited purposes
•   Adequate, relevant and not excessive
•   Accurate
•   Not kept longer than necessary
•   Processed in accordance with the data subject's rights
•   Secure
•   Not transferred to other countries without adequate protection

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
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.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:
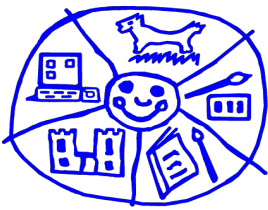•   Establish the facts
•   Ascertain compliance with regulatory or self-regulatory practices or procedures
•   Demonstrate standards, which are or ought to be achieved by persons using the system
•   Investigate or detect unauthorised use of the communications system
•   Prevent or detect crime or in the interests of national security
•   Ensure the effective operation of the system
•   Monitoring but not recording is also permissible in order to:
•   Ascertain whether the communication is business or personal
•   Protect or support help line staff
•   The school reserves the right to monitor its systems and communications in line with its rights under this act

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study.

The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -
•   Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
•   Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes 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.

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.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

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. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
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. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.
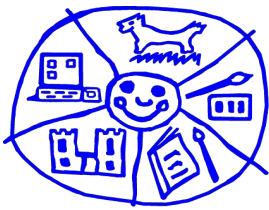
Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

• The right to a fair trial
• The right to respect for private and family life, home and correspondence
• Freedom of thought, conscience and religion
• Freedom of expression
• Freedom of assembly
• Prohibition of discrimination
• The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

MODEL POLICY/GUIDANCE ON THE USE OF SOCIAL NETWORKING SITES
(to be read in conjunction with E-Safety Policy)

General

This policy on social networking websites is in addition to the School's existing policy on email and internet use or Acceptable Use Policy. It takes account of the ACAS guidance on Social Networking.

In this policy 'staff' means employees, volunteers (including Governors, Trustees or Directors), agency staff or anyone working within the school and using the school's IT equipment.

In addition, other relevant professional standards, principles and codes of conduct applied by the school will sit alongside this policy. These include *(Insert/delete as appropriate: Teachers' Standards, National Occupational Standards for Supporting Teaching Learning and the 'Nolan Principles'.)* The school expects all staff to abide by these standards, as applicable to their role.

As staff are aware, access to the internet via the school's IT equipment is provided (primarily) for school use. We recognise however, that many employees may occasionally access the internet for personal purposes while in school. We also recognise that many employees participate in social networking on websites such as Facebook, Twitter, MySpace, Bebo and Friendster outside of work.

The purpose of this policy is to outline the responsibilities of staff using the internet to access social networking websites. This policy applies to all staff using the school's IT equipment.

Personal use of the internet

The school restricts and monitors access to social networking websites from its computers at all times. Access will only normally be allowed where use of such websites is for school purposes.

Personal conduct

The school respects staff's right to a private life. However, the school must also ensure that confidentiality with regard to its pupils, employees, volunteers, and its reputation are protected. It therefore requires staff using social networking websites to:
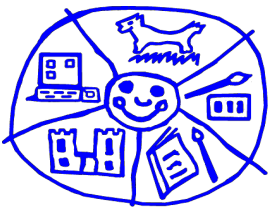
- use caution and act responsibly when posting information on social networking sites and blogs
- refrain from identifying themselves as working for or in any other way connected to the school
- ensure that they do not conduct themselves in a way that conflicts with their professional code of conduct, or is otherwise detrimental to the school; and
- take care not to allow their interaction on these websites to damage working relationships between members of staff, pupils at the school and their families, and other stakeholders or working partners of the school.

If staff become aware of inappropriate material/comments they should notify the Headteacher as soon as possible, and if possible provide print outs of the comments made or of the pictures displayed.

Staff must not be 'friends' or communicate with, students on any social network sites or similar websites, including, but not limited to, 'Facebook', 'Myspace', 'Twitter' etc. If any student makes contact with any staff member, they must notify the Headteacher as soon as possible without making a response. Similarly, if any member of staff or individual associated with the school makes unintended contact with a pupil, this must be notified to the Head Teacher as soon as possible. In the absence of the Head Teacher, the Deputy or Assistant Head or a member of the SLT must be contacted. The Headteacher can then deal with the situation as appropriate.

Staff are reminded that bullying and harassment against any other member of staff via social media sites is taken as seriously as workplace bullying and harassment. Any allegations will be dealt with under the schools' normal bullying and harassment or disciplinary policies, as appropriate and may also be treated as a criminal offence.

Employees that post defamatory statements that are published on the internet may be legally liable for any damage to the reputation of the individual concerned. As a representative of the school, any statement made by employees could mean the school is vicariously liable for those statements if done in the course of employment, even if performed without the consent or approval of the school. The school takes these acts seriously and disciplinary procedures will be invoked if any such defamatory statements are made by its employees, which may lead to dismissal.

In the case of Governors, Trustees or Directors and volunteers, whilst these individuals are not subject to disciplinary procedures, advice and guidance will be taken as necessary, in relation to referral and sanctions under appropriate governing body procedures.

Monitoring of internet access at work

The school reserves the right to monitor staffs' internet usage, but will endeavour to inform an affected individual when this is to happen and the reasons for it. We consider that valid reasons for checking a member of staff's internet usage include suspicions that they have:
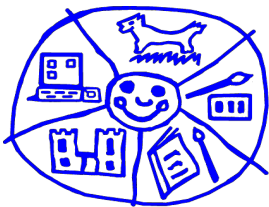
- been spending an excessive amount of time viewing websites that are not work-related; or
- acted in a way that damages the reputation of the school and/or breaches confidentiality
- contravened safeguarding policies or given cause for concern about their suitability to work with children

The school reserves the right to request information regarding members of staff's use of the internet from our Internet Service Provider (ISP).

Disciplinary action

If the school monitors staffs' internet use to ensure that it is in accordance with this policy, access to the web may be withdrawn in any case of misuse of this facility.

If appropriate, disciplinary action will also be taken in line with the school's disciplinary policy.

Security and identity theft

Staff should be aware that social networking websites are a public forum, particularly if the individual is part of a "network". Staff should not assume that their entries on any website will remain private. Staff should never send abusive or defamatory messages.

Staff must also be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords. In addition, staff must:

- ensure that no information is made available that could provide a person with unauthorised access to the school and/or any confidential information; and
- refrain from recording any confidential information regarding the school on any social networking website.
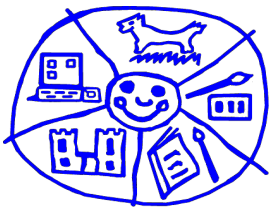
Any information posted on social network sites should be assumed to be in the public domain and this will be assumed in all cases of breach of the policy.

We ask all staff to consider the following before posting information or images on social networking sites:

- Think carefully before posting information – would you want your employer or a potential employer to see it?
- Think carefully about who might see it, i.e. parents, pupils, the wider community, and what you do and don't want them to see
- Review your information regularly and do not post information 'in the heat of the moment' – what may have seemed like a good idea at the time may not seem such a good idea the next day or some months or years later.

Glossary of Terms

AUP   Acceptable Use Policy – see templates earlier in this document
Becta   British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology)
CEOP   Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes
CPD   Continuous Professional Development
CYPS   Children and Young Peoples Services (in Local Authorities)
DCSF   Department for Children, Schools and Families
ECM   Every Child Matters
FOSI   Family Online Safety Institute
HSTF   Home Secretary's Task Force on Child Protection on the Internet
ICO   Information Commissioners Office
ICT   Information and Communications Technology
ICTMark   Quality standard for schools provided by Becta
INSET   In Service Education and Training
IP address   The label that identifies each computer to other computers using the IP (internet protocol)
ISP   Internet Service Provider
ISPA   Internet Service Providers' Association
IWF   Internet Watch Foundation

JANET   Provides the broadband backbone structure for Higher Education and for the National Education Network and RBCs

KS1   Key Stage 1 (2, 3, 4 or 5) – schools are structured within these multiple age groups eg KS3 = Years 7 to 9 (age 11 to 14)

LA   Local Authority

LAN   Local Area Network

Learning Platform   A learning platform brings together hardware, software and supporting services to support teaching, learning, management and administration

LSCB   Local Safeguarding Children Board

MIS   Management Information System

MLE   Managed Learning Environment

NEN   National Education Network – works with the Regional Broadband Consortia (eg Bungay High School) to provide the safe broadband provision to schools across Britain

Ofcom   Office of Communications (Independent communications sector regulator)

Ofsted Office for Standards in Education, Children's Services and Skills

PDA   Personal Digital Assistant (handheld device)

PHSEE   Personal, Health, Social Economic Education

RBC   Regional Broadband Consortia (eg Bungay High School) have been established to procure broadband connectivity for schools in England. There are 10 RBCs covering 139 of the 150 local authorities

SEF   Self Evaluation Form – used by schools for self-evaluation and reviewed by Ofsted prior to visiting schools for an inspection

SRF   Self Review Form – a tool used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark

South West Grid for Learning – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW

TUK   Think U Know – educational eSafety programmes for schools, young people and parents.

VLE   Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP   Wireless Application Protocol

Updated May 2012
Reviewed by E-Safety Committee on 17th May 2012
Adopted by full Governing Body 4th July 2012