King Offa Primary Academy
Acceptable Use Policy AY2020-2021

1. BACKGROUND

1.1 This acceptable use policy ("**AUP**") describes acceptable use of the Services by the Service Aggregator (**"Connecting Organisation"**), which connect to the Services for the purpose of providing educational, governmental and other related services to pupils (**"Users"**).

1.2 Use of the Internet and Services, such as the electronic mail service, are primarily intended for educational and government purposes only. [The Services may not be used for commercial or financial gain without obtaining prior express written approval from the Service Provider].

1.3 The Service Provider recommend that Internet use in educational establishments is driven by clear learning intentions that are set in the context of well framed tasks.

1.4 It is the responsibility of the Connecting Organisation to ensure that its employees and all Users are required to follow all the conditions laid down in this AUP.

1.5 Connecting Organisations must have in force an acceptable use policy in terms which comply with this AUP which employees of the Connecting Organisation, and Users (and where a User is below the age of sixteen, the User's legal guardian) are fully aware of in order to regulate the use of the Internet via the Services, and which seeks to enforce all of the conditions which are laid down in this AUP.

2. ACCEPTABLE INTERNET USE GUIDELINES

2.1 Use of the Internet outside of the scope of this AUP (as set out in paragraph 1.2) should be agreed [within the Connecting Organisation] and will be subject to the same guidelines and policies as though the User is using the Services for the purposes set out in paragraph 1.2.

2.2 Use of the Internet by Users must be supervised by an appropriate employee of the Connecting Organisation, and the Connecting Organisation must take steps to monitor, and where appropriate, record this usage.

2.3 The Connecting Organisation must ensure that access by Users who are under the age of sixteen should always be in areas where screens are visible to the supervising employees of the Connecting Organisation.

2.4 Connecting Organisations must ensure that Users are not given access to newsgroups or 'chat areas' unless using areas specifically designed for safe use and they are supervised by an appropriately qualified employee of the Connecting Organisation.

2.5 Connecting Organisations must ensure that Users do not give out personal details over the Internet except in circumstances (e.g. joint projects), which the Connecting Organisation has approved. The Service Provider recommends that 'Web names' are a useful way of shielding real identities.

2.6 Connecting Organisations must keep its anti-virus software up to date and comply with the obligations set out in paragraph 8 of this AUP to ensure that activities are not disrupted by malevolent actions by others.

2.7 Employees of Connecting Organisations receiving questionable materials should report these immediately to the appropriate member of their organisation.

2.8 All Connecting Organisations must make Users aware that all access is logged, and that any material accessed may subsequently be viewed by other Users as well as being monitored by the Connecting Organisation and/or the Service Provider system administrator.

2.9 Connecting Organisations must ensure that its personal computers (including portables) may only be used to access the Services using the mandated routing (the technical configuration which will be dictated through the site's use of the USO support site) and inter site policies.

2.10 Any software downloaded from the Internet by the Connecting Organisation or any User must be appropriately virus checked, licensed and registered.

3. UNACCEPTABLE USAGE GUIDELINES FOR THE INTERNET

3.1 It is contrary to this AUP for any Connecting Organisation to allow its employees or users to use the Services for any of the prohibited acts (**"Prohibited Acts"**) set out in paragraphs 3.1.1 to 3.1.14 below. Each of the Prohibited Acts, whether carried out by an employee of a Connecting Organisation or a User, may lead to a termination of the Connecting Organisation's agreement with the Service Provider for connection to the Services:

3.1.1 access to or creation, transmission or publication of any offensive, obscene or indecent images, sounds, data or other material;

3.1.2 a breach of confidentiality that results in information being inappropriately displayed or made available to others;

3.1.3 access to or creation, transmission or publication of any data capable of being displayed or converted to such obscene or indecent images, sounds, data or other material;

3.1.4 the creation, transmission or publication of any material which is designed or likely to cause offence, inconvenience or needless anxiety;

3.1.5 the creation, transmission or publication of defamatory, violent, abusive or homophobic material;

3.1.6 receipt or transmission of material such that this material infringes the copyright of another person;

3.1.7 transmission of unsolicited commercial or advertising material to other users of the Internet or any other network reachable via the Internet;

3.1.8 deliberate unauthorised access to facilities, services, data or resources within the Connecting Organisation, any other network or service accessible via the Internet;

3.1.9 deliberate activities with any of the following characteristics or that by their nature would result in:

3.1.9.1 wasting the Connecting Organisation's employees or other Users efforts or network resources, including time on remote systems and the efforts of the Connecting Organisation's employees involved in the support of those systems;

3.1.9.2 corrupting or destroying other Users' data;

3.1.9.3 violating the privacy of other Users;

3.1.9.4 disrupting the work of other Users;

3.1.9.5 using the Internet in a way that denies service to other Users (for example, by overloading the connection to the network by unnecessarily, excessively and thoughtlessly downloading or uploading large files);

3.1.9.6 continuing to use any item of software after being requested to cease its use because it is disrupting the correct functioning of the Connecting Organisation's network or the Internet (for example, utilities designed to broadcast network-wide messages);

3.1.10 malicious, willful or reckless use of the Internet having the intent or the effect to:

3.1.10.1 gain unauthorised access to computer material;

3.1.10.2 gain unauthorised access to computer material with the intent to commit or facilitate the commission of any further offence;

3.1.10.3 demand material from a user of another computer system;

3.1.11 the introduction of viruses;

3.1.12 where the Internet is being used to access another network, any abuse of the acceptable use policy of that network;

3.1.13 any use of the Internet that would bring the name of the Connecting Organisation and/or the Service Provider into disrepute; or

3.1.14 purchasing or ordering items on the Internet without the appropriate authorisation or due regard to the financial policies and procedures of the Connecting Organisation.

4. DATA PROTECTION

4.1 The Connecting Organisation must ensure that receipt or transmission of material by its employees or any User:

4.1.1 should not disclose the identity of any living person without that person's consent;

4.1.2 which identifies a living person should not be transmitted outside the European Economic Area unless it is to a country that has in place laws to protect the confidentiality, security and use of that information that equate to those found in the European Economic Area or under the terms of a written agreement that provides such protection. In either case that person's consent is required.

5. LIABILITY

5.1 Connecting Organisations are solely responsible and the Service Provider, accepts no liability for the use, content and messages that a Connecting Organisation, its employees or Users post, distribute or otherwise make available using the Services.

5.2 The Service Provider accepts no liability for any orders for goods and/or services, which a User places over the Internet when using the Services.

5.3 The Connecting Organisation's agree to indemnify the Service Provider against all claims, losses, liabilities, costs (including legal costs) and expenses which the Service Provider may incur as a result of the Connecting Organisation's breach of your obligations in this AUP or the use or misuse of the Services.

6. INFORMATION ON THE WORLD WIDE WEB

6.1 Connecting Organisation's are reminded that publishing material on the world wide web makes it widely available and that as such due care and diligence must be taken by the Connecting Organisation to ensure that any communication via this medium by the Connecting Organisation, its employees or its Users is regulated.

6.2 Connecting Organisations are advised when designing web sites to avoid publishing pictures of individual pupils with personal information about them. This will ensure that their privacy is protected and ensures that strangers will not be able to approach them outside school with information they have taken from the Connecting Organisation's web site. Where decisions are made to include images of individual children under the age of sixteen then this must be authorised by the legal guardian of the child.

6.3 One or more employees of the Connecting Organisation should take responsibility for vetting data before it is uploaded to a Service Provider web site to ensure the data is in line with local policies and best reflects the character of the Connecting Organisation. As part of this process the Connecting Organisation will also be responsible for ensuring that the ownership, accuracy and copyright of the material are appropriate prior to publication.

6.4 The web site should reflect the work of the Connecting Organisation and web authors should attempt to seek contributions from all teachers, year groups, head teacher, governors, parents and the local community.

6.5 Most good web publishing software have spellcheckers. It is advisable to ensure that work is spell checked before uploading to a server or the portal.

6.6 Users are encouraged to write material in ‘plain English’

6.7 When using images from other sites it is advisable to seek permission first. This can

be done by sending an email to the contact name on the web site. Connecting Organisations are reminded of their obligation in paragraph 3.1.6.

6.8 Connecting Organisation's should note that any data originating from their organisation or relating to business conducted by, or on behalf of them, and which is transmitted by the Internet remains the property of the Connecting Organisation and that the copyright or other intellectual property rights attached to that data are unaltered in any way.

6.9 The Connecting Organisation must respect the privacy and confidentiality of any data or other material published on the Internet and must be mindful that same restraints apply to the Internet based communication as to any other medium.

6.10 The Service Provider recommends that each page of the web site should be consistent in terms of design, layout, graphics and fonts. This will make it easier for Users to read and navigate the site.

7. GUIDELINES FOR ELECTRONIC MAIL USE

7.1 Connecting Organisations must abide by the following code of conduct.

7.2 Connecting Organisations must:

7.2.1 ensure that procedures are in place to ensure that inbound and outbound mail is virus free, and ideally, can identify and block the transmission of unsuitable information.

7.2.2 encourage its employees and Users to regularly housekeep e-mail deleting mail that is no longer required;

7.2.3 not, and ensure that its employees and Users do not, transmit personalised or financial data over the Internet unless it is encrypted or appropriately scrambled;

7.2.4 report and ensure that its employees and Users report unsolicited mail (“spamming”) to Schools.ICTServices@eastsussex.gov.uk.

7.2.5 ensure that its employees and Users do not delegate digital signatures or electronic pin numbers / identifiers to colleagues;

7.2.6 ensure that its employees and Users make arrangements for ensuring that e-mail is forwarded to a trusted colleague in an employee's or User's absence to ensure that important messages and transactions are not lost. (However, Users and employees of Connecting Organisations should NEVER redirect mail without advising such colleagues first!);

7.2.7 encourage its employees and Users not to print e-mail unnecessarily, as this will minimise the environmental benefits of using electronic communication. (The exception is e-mail that may be used in legal proceedings which should be printed off as mail administrators may have procedures which automatically remove mail that has been read after a set number of days);

7.2.8 discourage inappropriate use of the carbon copy function by its employees and its Users. Mail should only be copied to those parties that have been involved in previous communication and need to be involved in the communication process;

7.2.9 discourage employees and Users from sharing common mail accounts;

7.2.10 ensure that its employees and Users clearly identify confidential mail items as such (e.g. in the subject field);

7.2.11 encourage employees and Users to carefully check emails before sending;

7.2.12 ensure that its employees and Users avoid expressing strong feelings of disagreement in public forums (use an individual's private mail box);

7.2.13 ensure that its employees and Users are made aware of copyrights and licences and are careful not to breach them;

7.2.14 ensure that its employees and Users ask permission before forwarding or copying other people's messages;

7.2.15 avoid and ensure that its employees and Users avoid sexist, racist, violent, abusive and homophobic language as would be expected in any other context;

7.2.16 ensure that its employees and Users avoid writing messages using ALL upper case letters;

7.2.17 ensure that if the message is very important, controversial or open to misunderstanding, the Connecting Organisation, its employees or any User must consider a face to face discussion or a telephone conversation instead;

7.2.18 ensure that its employees and Users select the right forum for discussion - private mail or conference;

7.2.19 ensure that it, its employees and Users, when joining a conference which has been in existence for some time, read through all the contributions to date to avoid asking a question or making a point which has already been made; and

7.2.20 Connecting Organisations should consider putting a standard disclaimer on e-mail;

7.3 To make sure messages are read the Connecting Organisation must encourage its employees and Users:

7.3.1 to make sure the title of a message is relevant and if starting a new topic, change the subject line;

7.3.2 to get to the point quickly, as this way more people will read the message;

7.3.3 to keep messages short; and

7.3.4 to use short paragraphs as they are easier to read on screen. Double line spaces between paragraphs help, and bulleted or numbered lists are a good

way to display separate ideas.

8. ANTI-VIRUS POLICY

8.1 Introduction

8.1.1 This policy document outlines responsibilities and methods for ensuring that Connecting Organisations do not jeopardise the integrity and security of the computer systems in the Services. All employees of Connecting Organisations should be aware of the guidelines and recognise that breaching them may result in disciplinary action by the Connecting Organisation.

8.1.2 Connecting Organisations must ensure that their systems are protected by anti-virus measures, that processes are in place to ensure the anti-virus systems are kept up to date in line with supplier recommendations and that the organisation has the technical capability to maintain its anti-virus system.

8.1.3 Malicious software can be categorised into five main types of code, namely viruses, logic bombs, trojan horses, worms and hoaxes:

8.1.3.1 Virus type code attaches itself to a program (as opposed to data) file on a disc, or onto the “boot sector” which is read by the PC when it first starts up

8.1.3.2 Logic bombs are activated when certain criteria are met, e.g. the date being Friday 13th;

8.1.3.3 Trojan horses are contained within, as opposed to attached to, existing software (including viruses) and cause extra instructions to be executed, for example copying usernames and passwords to a hidden file which the perpetrator can access later in order to breach security; and

8.1.3.4 Worm code is similar to virus code but is able to exist on its own (i.e. without being attached to another file). Worms replicate themselves, and then destroy the “mother copy”, which gives the impression that the software is moving about the disc, until the disc eventually fills up.

8.1.3.5 Hoax virus-warnings. These are messages sent out to users requesting that they warn (i.e. forward the message to) everyone in their address book and are based on similar principles as a chain letter.

8.2 Sources of Virus Infection

8.2.1 Research has shown that viruses tend to be written by pupils, computer hobbyists or disgruntled employees. The latter group directing their attacks specifically at their employer’s (or former employer’s) organisation.

8.2.2 The vast majority of viruses are unwittingly introduced to an organisation from an external source. Common routes are:

8.2.2.1 discs brought in from home;

8.2.2.2 unsolicited e-mails;

8.2.2.3 free software from PC magazines;

8.2.2.4 demonstration and evaluation software;

8.2.2.5 websites with malicious code on;

8.2.2.6 files and software downloaded from the Internet; and

8.2.2.7 engineer's discs.

8.2.3 Once introduced, viruses are easily transferred from one PC to another by means of a floppy disc or as email attachments.

8.3 Guidelines For Preventing Corruption Or Loss Of Data Through Computer Viruses

8.3.1 All Connecting Organisations must have anti-virus software installed and have procedures in place to keep the software up to date.

8.3.2 All new computers purchased must be certified virus-free on delivery.

8.3.3 All ICT contractors on a Connecting Organisation's site will be expected to work within the Service Providers guidelines and should use virus free software and disks.

8.3.4 The Connecting Organisation must have procedures in place for ensuring that anti virus software is updated on a regular basis.

8.3.5 All existing PC's must have recommended anti-virus software loaded and scanning enabled for both the hard drive and the floppy disk or USB sticks or other storage media devices.

8.3.6 Until such time as all PC's within a given area have anti-virus enabled, it is the responsibility of the Connecting Organisation to have a stand-alone PC available for the validation of all incoming discs and CD-ROMS.

8.3.7 PCs used from home to connect directly to the Services or resources within the Services must have anti-virus software loaded and scanning enabled.

8.3.8 All incoming discs must be scanned prior to loading either automatically or through the stand-alone system designated for this purpose.

8.3.9 Software must only be purchased from the approved suppliers or in accordance with Connecting Organisation procedures and must be certified virus-free.

8.3.10 Blank discs must only be purchased from suppliers who certify that they are virus-free.

8.3.11 Unsolicited or unauthorised software must not be loaded on the

Connecting Organisations computers.

8.4 **Elimination of Virus Infection**

8.4.1 On detection of a virus infection, employees of the Connecting Organisation must immediately take steps to contain the virus and prevent its spread outside the Connecting Organisation.

8.4.2 Any virus infections on the Connecting Organisation's System should be recorded. The record should contain the date of the infection, the virus encountered, the PCs affected and where possible identify the source of the virus.

8.4.3 The infected System must be immediately disconnected from the Services.

8.4.4 Disinfection of virus-infected Systems must only be carried out by suitably qualified employees of the Connecting Organisation.