



LET'S GET DIGITAL

ACCEPTABLE USE POLICY

1. BACKGROUND

- 1.1 This acceptable use policy ("**AUP**") describes the acceptable use of the Services by the Service User and each school for which it requires a connection to the Services pursuant to a Service Order.
- 1.2 For the purposes of this AUP, the Service User's schools and other end users of the Services, including the Service User where the context requires is referred to as an "**End User**".
- 1.3 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 by the Service Provider or any End User for commercial or financial gain without obtaining prior express written approval from the Service Provider.
- 1.4 It is the responsibility of the Service User to ensure that End Users comply with the conditions of this AUP. Accordingly, the Service User must have in force an acceptable use policy that complies with this AUP of which End Users (and where an End User is below the age of sixteen (a "**Minor**"), the End User's legal guardian) are fully aware and which enforces its conditions.

2. UNACCEPTABLE USE

- 2.1 End User must not use the Services for any of the following purposes ("**Prohibited Acts**"):
 - 2.1.1 access to or creation, transmission or publication of any offensive, obscene or indecent images, sounds, data or other material;
 - 2.1.2 access to or creation, transmission or publication of any data capable of being displayed or converted into obscene or indecent images, sounds, data or material;
 - 2.1.3 the creation, transmission or publication of any material which is designed or likely to cause offence, harm, inconvenience or needless anxiety;
 - 2.1.4 a breach of confidentiality that results in the unauthorised display or disclosure of information;
 - 2.1.5 the unauthorised disclosure of personal information relating to another person, including name, contact details, images, data or other material;
 - 2.1.6 the creation, transmission or publication of defamatory, violent, abusive or sexually discriminatory material;



- 2.1.7 transmission of material that infringes the intellectual propriety rights (principally but not limited to copyright) of another person;
- 2.1.8 transmission of unsolicited commercial or advertising material to other users of the Internet or any other network reachable via the Internet;
- 2.1.9 unauthorised access to computer systems or materials whether or not with the intension of committing or facilitating the commission of a criminal offence;
- 2.1.10 unauthorised access to computer systems or materials to intentionally or recklessly impair the operation of any computer system, prevent or hinder access to any application held on any computer system, or to impair the operation of any such application or the reliability of any data held on any computer system;
- 2.1.11 unauthorised acts that cause or create a significant risk of serious damage of a material nature to any computer system;
- 2.1.12 making, adapting, supplying or offering to supply a program or data for the commission or assistance in the commission of a criminal offence;
- 2.1.13 making intentional or reckless demands for money, information or other material from a user of a computer system, including by denying access to any application or data held on that computer system;
- 2.1.14 deliberate activities which, by their nature, would result in:
 - 2.1.14.1 wasting the efforts of the Service Provider, or network resources, including time on remote systems and the efforts involved in the support of those systems;
 - 2.1.14.2 corrupting or destroying other End Users' data or otherwise disrupting access to that data;
 - 2.1.14.3 violating the privacy of other End Users;
 - 2.1.14.4 disrupting the work of other End Users;
 - 2.1.14.5 using the Internet in a way that denies service to other End Users (for example, by overloading the connection to the network by unnecessarily, excessively and thoughtlessly downloading or uploading large files); or continuing to use any application after being requested by the Service Provider to cease its use because it is disrupting the correct functioning of the network or the Internet (for example, utilities designed to broadcast network-wide messages);
- 2.1.15 the intentional or reckless introduction of malicious computer programs, including computer viruses;



2.1.16 where the Internet is being used to access another network, any abuse of the acceptable use policy of that other network; any use of the Internet that would bring the name of the Service Provider into disrepute;

2.1.17 purchasing or ordering items on the Internet without the appropriate authorisation or due regard to the financial policies and procedures of the Service User; or failure to put procedures in place to ensure that inbound and outbound email is virus free and, ideally, that it can identify and block the transmission of unsuitable information.

2.2 The Service Provider may terminate the Agreement pursuant to clause 9.3 if the Service User or an End User carries out one or more of the Prohibited Acts.

2.3 Recommended guidelines for the acceptable use of email and websites are set out in the Appendix.

3. DATA PROTECTION

3.1 The Service User acknowledges and accepts that it is responsible for its compliance and the compliance of End Users with the Data Protection Legislation.

3.2 The Service User shall hold the Service Provider harmless for the failure of the Service User and/or its End Users to comply with the Data Protection Legislation.

4. LIABILITY

4.1 The Service User is solely responsible for, and the Service Provider accepts no liability for the use, content and messages that End Users post, distribute or otherwise make available using the Services.

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

4.3 The Service User shall hold the Service Provider harmless for the acts and/or omissions of the Service User and the End Users and their use or misuse of the Services.

APPENDIX – GUIDELINES FOR ACCEPTABLE USE WEB SITES

The Service User is reminded that publishing material on the Internet makes it widely available and that due care should be taken by the Service User to ensure that any publication by the Service User or its End Users is regulated appropriately.

The Service User is advised when designing websites to avoid publishing pictures of individual pupils with personal information about them. This will ensure their privacy is protected and reduces the opportunities for strangers to make unsolicited approaches using information gleaned



from the website. Decisions taken to include images of Minors should be authorised by the legal guardian of the Minor.

One or more employees of the Service User should take responsibility for vetting data before it is uploaded to a website to ensure the data complies with local policies and best reflects the character of the Service User. As part of this process, the Service User should ensure the appropriate licensing and accuracy of the material prior to publication.

The website should reflect the work of the Service User and web authors should attempt to seek contributions from all teachers, year groups, head teacher, governors, parents and the local community.

Most good web publishing applications include spellcheckers. Work should have the spelling checked before uploading to a website.

End Users are encouraged to write material in 'plain English'

Permission should be obtained before using images from other websites. This can be achieved by sending an email to the contact name on the website.

Data originating from the Service User or relating to its business that is transmitted via the Internet remains the property of the Service User and that the copyright or other intellectual property rights attached to that data continue to apply unaltered.

The Service User should respect the privacy and confidentiality of any data or other material published on the Internet and should be mindful that the same restraints apply to the Internet based communication as to any other medium.

It is recommended that each page of the Service User's websites should be consistent in terms of design, layout, graphics and fonts. This will make it easier for End Users to read and navigate the site.

EMAIL USE

The Service User should ensure that End Users abide by the following code of conduct.

The Service Users should:

- encourage End Users to regularly delete email that is no longer required;
- not, and encourage that End Users do not, transmit personalised or financial data over the Internet unless it is encrypted;
- encourage that End Users do not delegate digital signatures or electronic pin numbers / identifiers to another person;
- encourage that End Users make arrangements to forward e-mail to a trusted colleague in the End User's absence so that important messages and transactions are not lost. However, End



Users should not redirect mail without first advising the relevant colleagues;

- encourage End Users not to print e-mail unnecessarily to minimise the environmental burden of printing;
- discourage inappropriate or indiscriminate use of large circulation lists of emails. Email should only be copied to those parties who have been involved in previous communications and need to be involved in the communication process;
- discourage the sharing of common email accounts by End Users;
- encourage that End Users clearly identify confidential mail items as such (e.g. in the subject field);
- encourage End Users to carefully check emails before sending;
- encourage End Users to avoid expressing strong feelings of disagreement in public forums (use an individual's private mailbox);
- encourage that End Users are made aware of copyright and licences and are careful not to breach them;
- encourage that End Users ask permission before forwarding or copying other people's messages;
- encourage that its employees and End Users avoid writing messages using upper case letters (also known as 'flaming');
- encourage that if a message is very important, controversial or open to misunderstanding, the End User considers an alternative means of communication instead;
- encourage that End Users select the right forum for discussion; private mail or conference;
- encourage End Users, when joining an email chain, read through all prior contributions to avoid asking a question or making a point which has already been made; and
- the Service User should include a standard disclaimer on email footers.
- to make sure messages are read, the Service User should encourage End Users:
 - to encourage the title of a message is relevant and, if starting a new topic, change the subject line accordingly;
 - to get to the point quickly, as this way more people will read the message;
 - to keep messages short; and
 - 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.