This is JANET(UK)'s response to the Department for Business, Innovation and Skills consultation on Implementing the Revised EU Electronic Communications Framework. JANET(UK) is the operator of JANET, the UK's National Research and Education Network, that connects universities, colleges, research organisations and regional schools networks to each other and to the Internet. Since JANET is classed as a Private Electronic Communications Service, much of the consultation is not directly relevant to us. This response therefore concentrates on areas of the Directives that are relevant to the services that we and our customers provide over the network.

(Questions from 7 onwards appear to be numbered differently in the text of the consultation and the summary on pages 60-61. This response uses the numbering from the consultation text)

Q1-2 (Appeals): not relevant to JANET, as a private network

Q3-6 (Facilities Sharing): We note that the proposed powers would extend to all undertakings providing Electronic Communications Networks, not just public networks. However since JANET(UK) does not own its communications infrastructure but rents it from suppliers we would expect any requirements to provide information to be directed to them.

Q7 (Security and Resilience of Networks and Services): not relevant to JANET, as a private network

Q8 (Dissuasive Sanctions): not relevant to JANET, as a private network

Q9 (Universal Service Obligations): not relevant to JANET, as a private network

Q10 (Equivalence of Access for Disabled Users): not relevant to JANET, as a private network

Q11 (Breach of Personal Data and Penalties)

We note that the consultation differs from the Directive in stating that these duties will apply to *all* providers of electronic communications services, rather than only to *public* services as the Directive requires. However we do not in any case consider it either appropriate or necessary to create a separate data protection regime for providers of electronic communications services, since there is no evidence that such organisations present a particularly high risk to the privacy of personal data. Indeed the Directive itself foresees that the same provisions will, in due course, be extended to all organisations handling personal data. We therefore consider that the requirements of the Directive should be implemented as standard UK data protection law, covering all data controllers.

However we do consider that clarity is required on the scope of personal data protection for which network providers are responsible. They must not, as has sometimes been suggested in the past, be responsible for privacy breaches resulting from careless configuration or operation of users' computers.

In introducing a requirement to report breaches of personal data we believe it is vital to be clear that the purpose of reporting is to protect affected individuals, not to name and shame organisations that suffer breaches. We are therefore concerned that page 128 of the Impact

Assessment seeks to create a "dissuasive reporting regime". Treating reporting as a punitive measure will encourage organisations to conceal their problems, thus risking further harm to their customers. We believe that where punishment is appropriate it should be handled separately, through monetary or other penalties. Otherwise there is a serious risk that customers will be encouraged to move from organisations that obey the law – admitting their breaches and being blamed for them – to those that ignore it – concealing their breaches and escaping with an undamaged reputation.

Q12 (Cookies)

We note that commentators have come to completely opposed conclusions about this provision of the Directive: both that it effectively prohibits third party advertising or analysis and that it means no change to current practice. We therefore believe it is essential for the meaning of the UK transposition of the requirement to be clear.

We welcome the consultation's pragmatic approach of considering that a properly-informed customer can give consent through their browser settings so that websites do not need to create additional opt-in consent pages that would rapidly make the web unusable (or, as the consultation notes, drive users away from EC websites). However we believe that this approach needs to be applied consistently across Europe, otherwise websites that are legal in one country will be illegal in others. Such an outcome would create significant new barriers to electronic commerce within the EC: precisely the opposite of the Commission's desire in their revision of the Data Protection Directive.

Q13 (Impact Assessments): no comments

Q14 (General Comment)

We regret that the consultation paper fails to address a significant change in Article 13 of the revised Directive, on unsolicited e-mail. The previous Data Protection Directive (*Directive 2002/58/EC*) contained a serious omission, which was transposed into the UK's *Privacy and Electronic Communications (EC Directive) Regulations 2003*, in that it only prohibited sending unsolicited e-mails to the "subscriber" to an electronic communications service. In a typical home connection, where members of the household may have separate e-mail addresses, this means that the bill payer's own e-mail is protected from spam but those of other family members are not. The difference is, of course, even worse for a company, government department or college where there may only be one "individual subscriber" and hundreds or thousands of "users". The amendments to the Directive correct this, by extending the prohibition to e-mail addresses of "subscribers or users", thus ensuring that all accounts are protected. We urge the Department to make the same important change to the UK Regulations.