Warwickshire County Council

Corporate eSafety Policy for the commissioning and management of online services

This document's security classification is NOT PROTECTIVELY MARKED

Document Control

Title:	Corporate eSafety Policy
Issued by:	E Communications
Date:	15 April 2009
Author	Tim Dumbleton
Version:	1.0
Status:	Final version

Revision History

REVISION	DATE	REVISION STATUS
0.2	15 April 2009	Draft for Review
0.3	7 May 2009	Revised based on feedback from ESB and HR
1.0	20 July 2009	Provided to ESB for final sign-off. Amendment made to page 4 following advice from L&G

Document Review

REVIEWER	POSITION	DATE
E Communications Strategy Board	Corporate strategy board	27/04/09
Martyn Thompson	Deputy Head of Human Resources	22/04/09
John Parmiter	Head of ICT Development Service, CYPF	26/03/09
Sioned Harper	Solicitor, Law & Governance	14/07/09

Table of Contents

1 Introduction

Websites and other online services provide many opportunities to enable communication between the public, Council staff, Elected Members and partner organisations. Blogs, wikis, discussion forums, image sharing services, mobile access and social networking amongst other technologies provide new ways to engage services users and drive innovation in service delivery.

However, online communication also brings risks including contact with people who may wish to cause harm, cyberbullying through messages and images and access to obscene or offensive content. These risks are as relevant to online services provided by the Council as for any other public or private organisation.

Whilst the majority of current advice and evidence focuses on young people, it is important to note that **esafety issues can potentially affect all people who use online services**, for example:

- vulnerable adults who may be at higher risk of being persuaded to share sensitive personal information;
- professional staff who may be at risk of misrepresentation and malicious accusations through social networking;
- Elected Members who may be at risk of receiving abusive messages where sensitive policy decisions are discussed online.

Online videos provided by the Child Exploitation and Online Protection Centre (CEOP) and Childnet International illustrate some of the major risks and the damage caused by online abuse.

The guidance provided in this document will help to minimise the esafety risks associated with online communication. Risk cannot be removed entirely, but the Council has a duty of care to all of its service users to protect their safety as far as is reasonably practicable. This is as relevant in the online world as in the physical world.

2 Purpose

This policy is relevant to senior managers and operational managers involved in commissioning, developing and managing websites and other online services. **This policy is relevant to all services provided to any audience, not just those intentionally aimed at young people.**

The policy requirements set out below must be followed for any online service (existing or proposed) provided by the Council or in partnership with other organisations. This includes where services are hosted by or delivered by a third party on behalf of the Council. The policy applies to all online communication facilities whether they are for the public in general or for specific groups (for example through closed online areas).

Online communication facilities on centrally managed systems such as the Intranet and WeLearn will already operate according to these guidelines. Therefore, individuals or teams wishing to use these facilities will not need to address the guidelines. However, they will be advised by the relevant core team of their responsibilities.

This policy is most relevant to online services which provide:

- Online discussion forums,
- Online chat or instant messaging facilities,

- Blogging facilities,
- Wikis,
- And any other facilities which allow users to post comments or communicate with other users in any way.

Examples of online services include:

- Online discussion forums provided to consult with local communities;
- Blogs provided to inform the public about the work of the Council;
- Online discussion forums which are not provided on the Intranet but are aimed at Council staff and Elected Members.

These guidelines are based on guidance from the Warwickshire Safeguarding Children Board, the Home Office, the Child Exploitation Online Protection Centre (CEOP) and Childnet International and are in line with current guidance available from Becta on 'Safeguarding Children in a Digital World'.

Whilst much of the available guidance has been developed for services aimed at young people, the principles and good practice apply to uses with all age groups and audiences.

These guidelines should be used in conjunction with Council briefing notes on information security and data protection available on the Intranet and the Social Networking Policy. Corporate branding guidelines must also be addressed.

3 Scope

This policy covers the use of all websites and online services managed and developed by or on behalf of the Council. Online services (such as WeLearn) provided to support schools and other formal education providers are not covered by this policy as they will already have appropriate guidance and policies in place.

4 Enforcement

Any breach of the terms set out below could result in the application or offending content being removed in accordance with the published complaints procedure and the publishing rights of the responsible Council representative being suspended.

The E Communications team reserves the right to require the closure of any applications or removal of content published by Council representatives which may adversely affect the reputation of the Council or put it at risk of legal action.

Any actions, communications or content that cause damage to the County Council, any of its employees or any third party's reputation may amount to misconduct or gross misconduct to which the County Council's Dismissal and Disciplinary Policies apply.

The Council will also co-operate fully with investigations where extreme cases of online abuse warrant involvement of external enforcement agencies.

5 Related Documentation

This policy refers to and should be read in conjunction with the following documents:

Document Description	Type
Use of social networking applications as part of Council services: guidance	Guidance
Social Networking Policy	Policy
External Links Policy	Policy
Information Security Policies	Policy
Corporate Identity Manual	Policy

6 Policy

The following guidance must be followed when new online services are being considered. It must also be retrospectively addressed by any existing online services which provide communication facilities.

6.1 The E Communications Manager must be informed of any proposals to develop new online services. It will be preferred that, where possible, proposals make use of existing online facilities available to the Council that are relevant to the audience group.

6.2 Proposals must only be taken forward where it has been agreed with relevant Head of Service and the E Communications Manager. Proposals which are deemed to present unreasonable levels of risk or duplicate existing facilities are unlikely to be taken forward. In cases where this cannot be decided by the Head of Service or Service Manager and the E Communications Manager, the proposal will be referred to the E Communications Strategy Board.

6.3 A risk assessment must be carried out to establish which features may present risks and how they should be managed. The checklist provided in the Appendix (page 64) to the Home Office's Good practice guidance for the providers of social networking and other user interactive services 2008 should be used to carry out the risk assessment. The E Communications team can also advise on carrying out risk assessments of this type.

6.4 Named contacts for the following roles must be identified, documented and kept up to date. The E Communications team must also be provided with this information. Roles which must be addressed include:

- The responsible Head of Service
- The service or operational manager who will have day to day responsibility
- Members of staff involved in the administration of the online service
- Contacts in partner organisations or third parties which will have a role in providing the online service.

6.5 Formal roles such as online facilitation or moderation should not be undertaken by members of the public or organisations with no formal involvement in service delivery. However, there may be exceptional circumstances where this is appropriate but this must only be done with the agreement of the E Communications Manager.

6.6 Proposals must clearly address the following requirements:

- That any background checks and processes required under the Safeguarding Vulnerable Groups Act 2006 will be satisfied and relevant information recorded by the appropriate manager. This is particularly relevant to any

services aimed at children, young people and vulnerable adults. Further guidance regarding Criminal Records checks is available from Managing People under Safer Recruitment and Selection.

- Where a third party system is to be used, that all terms of use relating to that third party system are compatible with the proposal.
- Where online communication will be aimed at or accessible to children and young people, that their profile information are set to private by default, or that clear guidance is provided to users to encourage them to set information to private.
- That the guidance provided in Part 2 of the Home Office's Good practice guidance must be addressed satisfactorily.

6.7 Proposals must outline how online communication will be managed. This information should address:

- How communications (such as blog comments and forum postings) will be moderated, how frequently this will be done and what facilities will be in place to enable effective moderation (such as blocking and banning features).
- What terms and conditions of use will be applied to public users, Council users and any other potential users.
- What facilities will be available to enable users to make complaints or alert moderators to potential issues. The E Communications Manager may also recommend that the 'Report Abuse' button provided by CEOP should be included in services in addition to complaints and alerting mechanisms provided by the Council. Further information about requirements of complaint processes is provided in the document 'Use of social networking applications as part of Council services: guidance'.
- What facilities will be available for users to manage their communication, such as features to block other users' messages and to hide personal information from other users.
- What processes will be used to escalate, investigate and address complaints.

6.8 Managers must ensure that guidance appropriate to the target user groups is developed and promoted to encourage users to follow good practice and act responsibly. Guidance should mirror existing sources such as the Warwickshire Safeguarding Children Board's E-Safety Information Booklet. The E Communications team can advise on other suitable sources of advice.

6.9 Managers must ensure that corporate security standards for the handling, storage and disposal of personal data are addressed. This includes ensuring that the service is provided on servers with appropriate security features whether it is hosted within the Council or by a third party. Managers must consult the E Communications Manager and the ICT Security Manager regarding security requirements.

6.10 Managers must ensure that appropriate training is provided and background checks are carried out and recorded where relevant. The E Communications Manager can provide advice regarding circumstances where specific training and background checks are appropriate.

6.11 Managers must ensure that content under the control of the Council is created and maintained according to the Corporate Branding guidelines and content quality standards published in the Communications Toolkit section of the Intranet.

6.12 Managers must ensure that corporately agreed terms of use, data protection and Freedom of Information statements are used or incorporated in to statements provided to users.

6.13 Day to day management should be carried out in line with the processes outlined in 6.7 above and the good practice set out in Part 2 of the Home Office's Good practice guidance. All staff involved in the day to day running of online communications must be made aware of this guidance.

6.14 The manager and team responsible for the online service must ensure that new messages and other content submitted by users are checked at appropriate intervals. If checking of messages and other content cannot be maintained at an appropriate frequency, then the service may need to be reviewed as this will introduce e-safety risks and poor customer service.

6.15 All Council staff and Elected Members (whether directly involved in delivery or as other users of the service) must abide by the Social Networking Policy and must also act within the principles of the Corporate Governance Code.

6.16 All Council staff and Elected Members using the online service in a professional capacity must provide their full name, Council position and Council email address where the option to set up user profiles is available. This will reduce confusion between people's professional and personal use of the same service. Further information about these requirements is provided in the document 'Use of social networking applications as part of Council services: guidance'.

If you are in any doubt about any of the requirements outlined above, contact the E Communications Manager for further advice. Misuse of online communications can have serious consequences – it is better to clarify any questions rather than make assumptions.