Diocese of Elphin – HR Policy Handbook

Document Name: **Internet Policy**
Document No: **3.1.5 (original)**
Effective Date: **15th February 2019**
Written By: **Frank Mitchell, HR Advisor**
Approved By: **+Kevin Doran, Bishop of Elphin**

Operating under the patronage of Our Lady of the Immaculate Conception, the Diocese of Elphin aims to provide staff members with a safe, caring and supportive Christian environment in which to carry out their work. Work objectives are to be advanced with due regard to the needs and dignity of each staff member and with due regard for the individuals and communities the diocese serves.

This document outlines the Diocesan policy on Internet use. It is applicable to parishes, offices, agencies and any entity operating under the governance of the Diocese of Elphin (hereafter referred to as "the employer"). Line Managers (Bishop, Priests, Deacons, Religious, Lay Personnel who supervise staff members) are responsible for communicating this policy and having it signed off by their staff member(s).

The internet is a vital resource for the business of "the employer". However, the internet suffers from significant and widespread security and integrity risks and has the potential to be used in ways that are inappropriate to the aims and goals of "the employer". Therefore, the use of the internet is regulated by standards of acceptable use, as set out in this policy.

Access to the internet
All connections to the internet on computers provided for work purposes by "the employer" must be through an approved internet service provider (ISP). Access to the internet is to be limited to matters that are relevant to your work. Internet access for recreational or private purposes is not permitted (except as provided for below). Your use of the internet must at all times comply with the rules outlined in this policy.

Browsers
Software is required for browsing the internet. This software is installed on computers by approved suppliers. Only approved software may be used to access the internet on the computers provided for work purposes by "the employer".

Password access
All staff are issued with individual usernames and passwords for computers provided for work purposes which in turn grants access to the internet. Passwords must always be kept private and must not be shared, written down or disclosed on any internet site.

Monitoring access
Access to the internet from computers provided for work purposes is managed by "the employer". All incoming and outgoing traffic may be monitored for performance analysis and for other appropriate purposes. This traffic analysis shows date and time of internet access, user name, sites visited, and requests for information. This analysis will be used to identify areas of non-compliance with this policy. Appropriate action will be taken where necessary.

Appropriate use of the internet
All internet connections are intended for activities that either support "the employer's" business, or the professional development of staff. Use of the internet is to assist staff to achieve stated goals and objectives. This may include use of email, search engines (eg. Google, Yahoo, etc), and file transfer. All staff have a responsibility to use the internet in a professional, ethical and lawful manner at all times. Legal and contractual requirements concerning the intellectual property rights of outside parties must be strictly adhered to.

Diocese of Elphin – HR Policy Handbook

Document Name: **Internet Policy**
Document No: **3.1.5 (original)**
Effective Date: **15th February 2019**
Written By: **Frank Mitchell, HR Advisor**
Approved By: **+Kevin Doran, Bishop of Elphin**

Computer software must not be downloaded from any other source, without prior approval of your manager. The integrity of critical software will be reviewed on a regular basis and the presence of unauthorised files or amendments formally investigated.

You must at all times respect copyright and intellectual property rights of information you encounter on the internet. This may require obtaining appropriate permission to make use of information. You must always give proper credit to the source of the information used for "the employer's" purposes.

Material in which "the employer" has a proprietary interest – such as software, documentation or other internal information – must not be transmitted, sold or otherwise transferred to any outside party, except in pursuance of "the employer's" legitimate interests. Any departure from this policy requires the written authorisation of your manager. Misuse of internet facilities and services is prohibited.

Inappropriate use of the internet

You are prohibited from accessing, requesting or sending sexual, pornographic, racist, profane, violent or other offensive material via the internet. You are prohibited from saving, downloading, transmitting or purposely viewing sexual, pornographic, racist, profane or other offensive material. You are prohibited from sending chain letters, other forms of mass mailing and spamming (sending unsolicited emails to a number of people).

Staff access to social media during working time is governed by the social media policy 3.1.3.

"The employer" reserves the right to remove without notice any files or data from its information systems, including any information it views as offensive or potentially illegal, regardless of its source.

Access to the internet from computer provided for work purposes must never be used:
- for personal gain or profit;
- to represent yourself as someone else;
- to post or download messages that will reflect poorly on "the employer's" name and professional reputation;
- to advertise, or otherwise promote, unauthorised or illegal activities;
- to promote or engage in any activity that is in competition with diocesan activities;
- to process the personal data of any person in a manner inconsistent with the data protection legislation requirements;
- to transmit confidential information without the approval of your manager.

You must not join mailing lists from your work email address or solicit/contribute information on the internet without express permission from your manager.

Inappropriate use of the internet from external computers

You are prohibited from using the internet on computers outside the workplace, where such use has the potential to affect negatively "the employer" or its staff. Examples of such behaviour include:
- publishing material that is defamatory, abusive or offensive in relation to any staff member, manager, office holder, parishioner or client of "the employer";
- using the internet in a manner that amounts to bullying or harassment;
- publishing any sensitive information about "the employer";

Diocese of Elphin – HR Policy Handbook

Document Name: **Internet Policy**
Document No: **3.1.5 (original)**
Effective Date: **15th February 2019**
Written By: **Frank Mitchell, HR Advisor**
Approved By: **+Kevin Doran, Bishop of Elphin**

- publishing material that might reasonably be expected to have the effect of damaging the reputation or professional standing of "the employer".

Security

The internet is not a secure medium. Access to the internet, no matter how well set up, always poses some security risks. Accordingly, virus scanning software is installed on computers provided for work purposes. Staff members must not provide or use their passwords in response to any unexpected internet request for a password. Staff members must not provide any information relating to "the employer's" network/computers to any outside party, whether through the internet or in any other way.

Reliability of internet information

There is no quality control process on the internet and a considerable amount of information published on the internet is outdated, inaccurate or deliberately misleading. All information obtained from the internet should be considered with caution until confirmed by a reliable source.

Impact on other users

When using the internet, please be aware of your impact on others. Intense browsing or downloading during peak usage periods can impact on other people's work.

Enforcement

Non-compliance with the general principles and conditions of this internet policy may lead to disciplinary action, up to and including dismissal.

This policy is not exhaustive. In situations that are not expressly governed by this policy, you must ensure that your use of the internet is at all times appropriate and consistent with your responsibilities towards "the employer". In case of any doubt, you should consult with your manager.

Personal use of the internet

A limited amount of personal use of the internet on computers provided for work purposes is permitted, provided the following rules are observed.
- Personal use must not occur during working time, but instead must occur during break time or before or after your normal working hours;
- Personal use must not interfere with your work commitments;
- Personal use, including any downloading of data for personal use, must comply with the requirements and general principles of this policy and all other security and data protection policies. In particular, the above provisions regarding "Inappropriate use of the internet" and "Security" apply to personal use, as well as normal business use.

Monitoring of internet usage will apply to personal use as well as normal business use.

For further information please contact:
> HR Advisor
> Elphin Diocesan Office
> St. Mary's
> Temple Street
> Sligo F91 KTX2
> Email: hr@elphindiocese.ie
> Mobile: 087 240 4882