**Fairisle Junior School**
**Acceptable Technology Use Policy**

**September 2024**

Fairisle Junior School believes in promoting and encouraging the use of computers and the facilities they provide such as e-mail, the Internet and the intranet for the benefit of the community and its employees. To facilitate maximum use and development of our computer facilities, whilst at the same time protecting its interests, all users of the school's computer hardware, software, systems and networks are required to comply with its acceptable use guidelines and relevant school policies.

Where users are provided with computers for use away from the school site, it is the user's responsibility to ensure that no unauthorised or inappropriate use (as defined in this policy) is made of that computer by them or any other person who has access to it.

## Personal Use of Equipment

Users may use Fairisle Junior School provided computer equipment for occasional personal purposes provided that this never:

- Takes place at the expense of contractual hours
- Interferes with Fairisle Junior School work
- Relates to a personal business interest
- Otherwise contravenes Fairisle Junior School's computer usage guidelines

The network manager is responsible for monitoring the use of school provided computer equipment for private use. Users spending what senior management considers excessive time on private use may have access to computer equipment withdrawn.

## Personal Use of Internet Access and Email

Users may use the Internet and e-mail for occasional personal purposes provided that this never:

- Takes place at the expense of contractual hours
- Interferes with Fairisle Junior School work
- Relates to a personal business interest
- Involves the use of news groups (e.g. instant messaging & chat rooms)
- Otherwise contravenes Fairisle Junior School's computer use guidelines

## Installation of Software

Users do not have the access rights to install software on school computers and should not attempt to circumvent this restriction. Only authorised software which the school is licensed to use should be installed by the network manager. Users should be aware that installing software licensed to the school on computers not owned by the school is a breach of copyright and is illegal.

**Internet Access away from the school**

Users may connect school provided computers to home networks (either wired or wireless) which give access to the internet and to the school's Virtual Private Network (VPN) through NetExtender. This should be done using the Windows network connections control panel and **not** by installing proprietary software (e.g. Service Provider software on free CDs). You should ensure that your home wireless connection has appropriate security encryption.

**Acceptable Behaviour when Accessing the Internet or Using e-Mail**

Like any form of communication, the Internet and e-mail facilities must not be used for:

- The creation, use, transmission or encouragement of material which:
    - is illegal, obscene, libellous or otherwise defamatory
    - is offensive, threatening or annoying to anyone
    - infringes another person's copyright anywhere in the world
    - transmits unsolicited commercial or advertising material
- Obtaining unauthorised access to the school's or the City Council's or another organisation's IT facilities
- Violating other people's privacy
- Using facilities which do not serve the school's business functions, such as inappropriate chat lines or similar services, e.g. Bulletin Boards or playing games
- Illegal activities including breaching the General Data Protection Regulations (GDPR), Computer Misuse, Obscene Publications Act and Design Copyright and Patents Acts
- Unauthorised downloading of copyrighted or confidential information
- Wasting network and staff resources
- Wilfully disrupting other users' work in any way, including by viruses or data corruption
- Expressing personal views which could be misinterpreted as those of the school or the City Council
- Expressing views which could make people vulnerable to radicalisation
- Committing the school or City Council to purchasing or acquiring goods or services without proper authorisation
- Financial gain

Members of staff must report any suspected misuse, whether accidental or deliberate. Where necessary, the City Council will advise on the correct course of action and may further investigate sites, possibly consulting the police. In any case hardware including the contents of files held electronically may be monitored at any time by the Headteacher.

**Social Networking Sites**

The school has an expectation that any use of social networking sites by staff, either on school computers **or otherwise**, does not bring the name of the school or any of its staff into disrepute. All staff are advised to set security and privacy filters on such sites appropriately to avoid making private details public. Staff should not accept contact from pupils via social networking sites under any circumstances. Under no circumstances should the school be mentioned (positively or negatively) on any social media, apart from on the school's own Twitter account and website.

**Offensive and Inappropriate Material**

The use of school supplied equipment to access, store, copy or distribute items which are inappropriate, offensive, libellous (or in some other way illegal) or may jeopardise security in any way is prohibited. Users should be aware that to do so could constitute a prosecutable offence under UK law.

**I have read and understood the Acceptable Technology Use Policy**

**Signed _____ (member of staff)**

**Print Name _____ Date _____**