Elmfield Rudolf Steiner School

IT Policy – Non-Pupils

Incorporating:

Acceptable Use of IT
Social Media Guidance
Use of Portable Devices
Taking and Storing Images of Children

Management of Acceptable Use of IT for Pupils

Issued by	School Lead
Last review	22/08/22
Approved by Council	Oct 22
Circulation	Elmfield Website Google Drive – Policies

Scope

This Policy covers the Acceptable Use of IT by Staff and is overarching. Access to the School's systems is not intended to confer any status of employment.

Online Behaviour

As a member of the School community, you should follow these principles in all of your online activities:

- The School cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Emails should be treated in the same way as any other method of written communication. Anything that is written in an email is treated in the same way as any form of writing. You should not include anything in an email which is not appropriate to be published generally. The School will take no responsibility for any offence caused by you as a result of downloading, viewing or forwarding inappropriate emails.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the School community (for example content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the School community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Using the School's IT Systems

Whenever you use the School's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access School IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the School's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, School IT systems.

- Do not use the School's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the School monitors use of the School's IT systems, and that the school can view content accessed or sent via its systems.
- If you leave a workstation for any period of time, you should take appropriate action. This will either be to log off or lock the workstation.

Passwords

Passwords protect the School's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

Use of Property

Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the IT Manager.

Use of School Systems

The provision of School email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff should keep their personal, family and social lives separate from their School IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the School's right to monitor and access web history and email use.

Use of Personal Devices or Portable Storage Items

Personal devices used within the School site, or connected to the School network, are subject to the same policies and procedures as the School's own computers.
Portable Storage Items are only used for items which are relevant to school work. Users must not knowingly introduce unauthorised personal devices.

Monitoring and Access

The School email and internet usage (including through School Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and School email accounts may be accessed by the School where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Compliance with Related School Policies

To the extent they are applicable to you, you will ensure that you comply with the School's Online Safety Policy.

Retention of Digital Data

All emails sent or received on School systems will be routinely deleted after seven years and email accounts will generally be closed and the contents archived within one year of that person leaving the School.

Any information from email folders that is necessary for the School to keep for longer, including personal information (e.g. for a reason set out in the School Privacy Notice), should be held on the relevant personnel file. Important records should not be kept in personal email folders, archives or inboxes, nor in local files. Hence it is the responsibility of each account user to ensure that information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the School's email deletion protocol.

Breach Reporting

The law requires the School to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the School regardless of whether the personal data falls into a third party's hands. This would include:

- Loss of an unencrypted laptop, usb stick or a physical file containing personal data;
- Any external hacking of the school's systems, e.g. Through the use of malware;
- Application of the wrong privacy settings to online systems;
- Misdirected post, fax or email;
- Failing to bcc recipients of a mass email; and
- Unsecure disposal.

The School must generally report personal data breaches to the ICO without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If staff become aware of a suspected breach, they must notify the Business Manager.

Data breaches will happen to all organisations, but the School must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The School's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data

breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy, but failure to report a breach will be a disciplinary offence.

Breaches of this Policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the School's usual applicable procedures. In addition, a deliberate breach by any person may result in the School restricting that person's access to School IT systems.
If you become aware of a breach of this policy, or you are concerned that a member of the School community is being harassed or harmed online you should report it as if it were a safeguarding matter. Reports will be treated in confidence wherever possible.

SOCIAL MEDIA POLICY FOR STAFF – SCHOOL AND PERSONAL USAGE

Introduction

Elmfield School recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Bebo, LinkedIn, Twitter and all other internet postings including blogs and wikis. It is also a valuable educational tool.

Purpose

This policy applies to the use of social media for School and your own personal purposes, whether during normal working hours or in your personal time. Its purpose is to help staff avoid the potential pitfalls of sharing information on such social media sites and should be read in conjunction with the Acceptable Use Policy for pupils.

IT Facilities

The policy applies regardless of whether the social media is accessed using the School's IT facilities and equipment or your personal equipment.

Ownership

All material posted to a school sponsored media site becomes the ownership of Elmfield. Individuals posting comments or materials here lose all subsequent rights to this material which may be disseminated by the school in whatever way it chooses.

Guiding Principles

Staff are required to behave responsibly at all times and adhere to the following principles:

1.1 You should not be "Friends" with, 'Followers' of, or connect with pupils on any social media network. It would be considered inappropriate to connect with pupils on a personal account. Depending on the circumstances, it may also be inappropriate to connect with parents, guardians or carers.

1.2 You must be mindful of how you present yourself and the School on such media. Staff are entitled to a social life like anyone else. However, the extra-curricular life of an employee at the School has professional consequences and this must be considered at all times when sharing personal information.

1.3 You should always represent your own views and must not allude to other people's personal views in your internet posts.

1.4 When writing an internet post, you should consider whether the contents would be more appropriate in a private message. While you may have strict privacy controls in place, information could still be shared by others. It is always sensible to consider that any information posted may not remain private.

1.5 You should protect your privacy and that of others by omitting personal information from internet posts such as names, email addresses, home or work addresses, phone numbers or other personal information.

1.6 You should familiarise yourself with the privacy settings of any social media you use and ensure that public access is restricted. If you are not clear about how to restrict access, you should regard all your information as publicly available and behave accordingly.

1.7 You must not post anything that may offend, insult or humiliate others, particularly on the basis of their sex, age, race, colour, national origin, religion, or belief, sexual orientation, disability, marital status, pregnancy or maternity.

1.8 You must not post anything that could be interpreted as threatening, intimidating or abusive. Offensive posts or messages may be construed as cyberbullying.

1.9 You must not post disparaging or derogatory remarks about the School or its Governors, staff volunteers, pupils or parents, guardians or carers.

1.10 You must not use social media in a way which could constitute a breach of any policies contained in this Employment Manual.

1.11 You must not post anything that could be interpreted as glorifying or supporting terrorism, extremism or organisations promoting terrorist or extremist views, or encouraging others to do so.

1.12 You must not represent your own personal views as those of Elmfield.

Removing Postings

You may be required to remove internet postings which are deemed to constitute a breach of this policy. If you fail to remove postings, this could result in disciplinary action.

Breach

A breach of this policy may be treated as misconduct and could result in disciplinary action including in serious cases, dismissal.

Monitoring

The School regularly monitors the use of the internet, social media and email systems to check that the use is in accordance with this policy. If it is discovered that any of the systems are being abused and/or that the terms of this policy are being infringed, disciplinary action may be taken which could result in your dismissal.

ACCEPTABLE USE OF MOBILE DEVICES

Personal Mobile Devices (Including Phones)

- The School allows staff to bring in personal mobile phones and devices for their own use.
- Staff should use their mobile phone in a way that in no way negatively impacts their work
- During lessons, or when engaged in their duties, staff should have their phones on silent and they should not be used
- Under no circumstances does the School allow a member of staff to contact a pupil or parent/carer using their personal device while in School. If this is necessary from home, then precautions should be made to hide the number from which you are calling
- The School is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the School community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the School community
- Users bringing personal devices into School must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (Including Phones)

- Staff who have been issued a School mobile device may use it as intended; this includes use of DATA (not all School SIMs have a DATA contract), social media access, contact groups such as WhatsApp, uploading of images, etc.
- Staff who have been issued a device are fully responsible for the device and any activity on that device. They must not loan any device to another individual unless under direct supervision

- Staff who upload images and content must be aware of the School's Privacy Note and will be made aware of any pupil whose family has requested that their image is not utilised by the School
- The sending of inappropriate text messages between any member of the School community is not allowed
- Where the School provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used – save emergencies in which case care should be taken to hide the number from which you are calling

TAKING AND STORING IMAGES OF CHILDREN

As per the Elmfield School Privacy Note, the School considers that it has a legitimate interest In:

> making "use of photographic images of pupils in School publications, on the School website and where appropriate on the School's social media channels."

In order to allow parents the option to opt out of this (reasonable use), we allow them to write to the School in order to request that this happen. Once the School is made aware, all staff would be advised.

Should any individual be engaged in an event where they are representing the School and there is national press, then we must ask permission from the parents.

MANAGEMENT OF ACCEPTABLE USE OF IT FOR PUPILS

Pupils and parents will be asked to sign up to the schools Acceptable Use of IT (Pupils) and the Acceptable Use of Mobile Phones (Pupils) as part of the joining process for the school.

These policies make no differentiation of the use of a pupil's mobile data (3G/4G/5G) and the schools' network. We expect the pupils to behave in the same manner regardless of their means of connecting to the internet. The only real differentiation is that we are better able to police activities on the school network.