Acceptable Use of ICT Policy and Social Media

Author/Edited By	Eve Forster
Review Body	Teaching staff
Approved	To be approved by Governing Body
Next Review Due	To be reviewed every three years

January 2018.

Introduction
This policy will define the acceptable use of ICT (Information and Communications Technology) within our schools and set out clear guidelines for all members of the school community. Its purpose is to minimise the risk to pupils of inappropriate contact from staff, to protect employees and schools from litigation and to minimise the risk to ICT systems.

The school community is defined as all those people (pupils, teaching staff, non-teaching staff, parents, visitors, governors, etc.) who engage in learning, teaching, managerial and supportive activities within the confines of the school.

ICT resources are defined as:

- Any form of computing device (for example, servers, work-stations, laptops, tablet computers, calculators, iPads, mobiles) irrespective of any form of network connection;
- Any form of peripheral device (for example, a printer, scanner, digital still or video camera, control box, digital projector, microscope) that can be connected to any form of computing device or network connection and is capable of transmitting, receiving or responding to received data;
- Any form of computer or peripheral media, be it fixed or removable (for example, hard disc, USB, Memory Card, CD-ROM, floppy disc) that can transmit or receive data to or from any form of computing, peripheral or network device;
- Any form of software (for example, computer programmes such as word processors and image manipulators, or data files that record text, databases, sound, images, etc) that is supplied on, or via, any form of media or transmission medium (for example, floppy disc, CD ROM or the internet).

User Responsibilities
The principles that are being applied are that members of the school community should:

- Behave at all times within the current legislation and the expectations of the school community;
- Only use school ICT resources to further curriculum, professional and managerial responsibilities or other uses that are sanctioned by the head teacher or governors;
- Make careful and considerate use of the schools ICT resources, report faults and work in a way that minimises the risk of introducing computer viruses to the system;
- Protect pupils in school from the harmful or inappropriate material accessible via the internet or transportable on computer media;
- Help children to use email and similar systems appropriately and anonymously;
- Recognise their responsibility to maintain the privacy of individuals;
- Know and abide by the schools acceptable use policy as it applies to them and people in their care.
- All users are expected to act in a responsible, ethical and lawful manner. Users should uphold privacy and confidentiality in accordance with the Data Protection Act 1998. New data protection laws – not taking data off site?
- Must take care not to breach another person's copyright, trademark or design, nor to publish any defamatory content.
- No one may use ICT resources in violation of license agreements, copyrights, contracts or national laws, or the Standing Orders, policies, rules or regulations of the school or the County Council.
- Users are required to protect their password and not share their account details with others for their use, nor utilise another users' account or misrepresent their identity for any reason. Users must not under any circumstances reveal their password to anyone else.
- No user shall access (e.g., read, write, modify, delete, copy, move) another user's personal electronic documents (including email) without the owner's permission or as allowed by this policy or by law.
- Users must not upload or download software on any device without the authorisation of the Headteacher.
- Users must take care to store sensitive information, e.g. pupil data safely and to keep it password protected, on all school systems, including laptops. New data protection laws – not taking data off site?

- No one may use ICT resources to transmit, download or upload any abusive, threatening, or harassing material, chain letters, spam, or communications prohibited by law. No one may abuse the policies of any newsgroups, mailing lists, and other public forums through which they participate from a school account.
- No one may knowingly or willingly interfere with the security mechanisms or integrity of ICT resources. No one may use ICT resources to attempt unauthorised use, or interfere with the legitimate use by authorised users, of other computers on internal or external networks. Access to networks will be monitored.
- Staff are reminded that through their use of social media they must not post anything which would bring the school into disrepute.

School Responsibilities
The Governing Body is responsible for ensuring that employees act in a lawful manner, making appropriate use of school technologies for approved purposes only. They request information about the use of the internet (by children and adults) on a termly basis. This information is gathered by the IT technician (currently JC Comtech)

The Headteacher and computing subject leader are responsible for maintaining an inventory of ICT equipment, a list of school laptops and to whom they have been issued.

If a member of school community has reason to believe that any ICT equipment has been misused and a member of the school community is in breach of this policy, they should consult the Headteacher and or subject leader. If the Headteacher believes that the matter needs external investigation (i.e. is a matter of Safeguarding) then they would contact the Local Authority Designated Officer (LADO). Alternatively they would contact HR for advice about disciplinary procedures. Internal school staff should not carry out any investigations either formal or informal unless authorised to do so.

Internet Access:
At the Three Rivers Federation we ensure that our pupils are protected from illegal and inappropriate material, as much as possible, by subscribing to a filtered internet provider especially for schools maintained by Updata and managed by JC Comtech. Occasionally, the protection mechanisms provided by the ISP provider fail, either because the offending web site is new and is not known by the protection mechanism, or because the mechanism itself has developed a fault. As a school we alleviate this problem by ensuring our pupils are monitored during internet activities and constantly maintain vigilance. <u>Pupils are not allowed on the internet or email facilities without adult supervision.</u>

Network connected devices must have school approved anti-virus software installed and activated. Users may not turn off anti-virus software. All users of ICT resources have the responsibility to take precautions to prevent the initial occurrence and subsequent spreading of a computer virus. No one may knowingly create, install, run, or distribute any malicious code (e.g. viruses, Trojans, worms) or another destructive program on any ICT resource.

The Law:
Within the terms of the Data Protection Act 1998, Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the County Council or school may record or inspect any information transmitted through or stored in its computers, including email communications and individual login sessions without notice when:

- There is reasonable cause to believe the user has violated or is violating this policy, any guidelines or procedures established to implement this policy.
- An account appears to be engaged in unusual or unusually excessive activity.
- It is necessary to do so to protect the integrity, security, or functionality of ICT resources or to protect the County Council or its partners from liability.
- Establishing the existence of facts relevant to the business.
- Ascertaining or demonstrating standards which ought to be achieved by those using the ICT facilities
- Preventing or detecting crime
- Investigating or detecting unauthorised use of ICT facilities
- Ensuring effective operation of ICT facilities
- Determining if communications are relevant to the business (for example, in the last resort where an employee is off sick or on holiday and business continuity is threatened)
- It is otherwise permitted or required by law.

Personal use and privacy

In the course of normal operations, ICT resources are to be used for business purposes only. The school permits limited personal use of ICT facilities by authorised users subject to the following limitations:

- Personal use must be in the user's own time and must not impact upon work efficiency or costs.
- The level of use must be reasonable and not detrimental to the main purpose for which the facilities are provided.
- Personal use must not be of a commercial or profit-making nature.
- Personal use must not be of a nature that competes with the business of the school or conflicts with an employee's obligations.
- The Data Protection and E-Safety policies must be adhered to.

MOBILE PHONE COMMUNICATION AND INSTANT MESSAGING

No children are allowed mobile phones in school.

- If a child requires a mobile phone before or after school the child may take the phone to the office to be securely locked away until the end of the school day.
- Staff are not to give their home telephone number or their mobile phone number to pupils.
- Staff are not to make use of pupils' mobile phone numbers either to make or receive phone calls or to send to or receive from pupils' text messages.
- Photographs and videos of pupils should not be taken with mobile phones.
- Staff should not enter into instant messaging communications with pupils.
- Mobile phone communication should be used sparingly and only when necessary, children should not be present unless necessary. All staff are encouraged to leave mobile phones, switched off in their bags which should be left in a classroom cupboard or other safe place during lesson times. If staff expect to receive a call during lessons time they should direct the caller to the school landline in the office. If/when the call is made the member of staff will be informed by the office and if necessary, given time to leave the classroom to return or take the call.
- The school permits the use of personal mobile phones on trips to contact the school if/when appropriate and necessary. ??? How does this work as we do not have a school mobile

SOCIAL MEDIA

Three Rivers Federation understands that social media is a growing part of life outside of school. We have a responsibility to safeguard our pupils against potential dangers when accessing the internet at school, and to educate our pupils about how to protect themselves online when outside of school.

Three Rivers Federation defines social media as any online platform that offers real-time interaction between the user and other individuals or groups including –

- Blogs
- Online discussion forums
- Collaborative spaces such as Facebook
- Media sharing services such as YouTube
- Micro-blogging applications such as Twitter

We would define 'member of the school community' as any teacher, member of support staff, pupil, parent/carer of a pupil, governor and member of the school kitchen staff.

Social media use – staff

- School social media passwords are kept in the office.
- Julia Humphrey is responsible for the Federation Twitter account
- Staff must not access social media during lesson times unless it is related to the learning activity
- Staff may use social media during their break times but not in front of pupils.
- Members of staff must not 'friend' or otherwise contact pupils or parents through social media. Do we need something about being friends with parents as some staff and parents are local?
- If pupils or parents attempt to 'friend' members of staff through social media they should ignore requests.
- Members of staff should avoid identifying themselves as an employee of the school on social media.
- Members of staff must consider carefully the content of anything they post online and refrain from anything which is damaging to the school or any of its staff or pupils
- Where teachers or members of staff use social media in a personal capacity, they should make it clear that their views are personal. Staff may 'like' and 're-tweet' but not tweet about the school from their personal account.
- Teachers or members of staff must not post any information which could identify a pupil, class or the school.
- Members of staff should not post anonymously or under an alias to evade the guidance given in this policy.
- Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal.
- Members of staff should be aware that if their out-of-work activity brings the school into disrepute, disciplinary action will be taken.
- Members of staff should regularly check their online presence for negative content via search engines.
- If inappropriate content is accessed online, an inappropriate website content report form should be completed and passed on to the Headteacher.
- Attempts to bully, coerce or manipulate members of the school community, via social media, by teachers and members of staff will be dealt with as a disciplinary matter.
- Staff members should use their school email address for school business and personal email address for their private correspondence; the two should not be mixed.

Social media use – pupils and parents/carers

- Pupils should not access social media during lesson time as the school does not advocate the use of social media sites for children in the primary age range. It is blocked anyway – do we need this?
- Breaches of this policy by pupils will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution, or exclusion.
- Pupils and parents/carers are requested not to attempt to "friend" or otherwise contact members of staff through social media. If attempts to contact members of staff through social media are made, they will be reported to the Headteacher.
- If members of staff attempt to "friend" or otherwise contact pupils or parents/carers through social media, they should be reported to the Headteacher.
- Pupils and parents/carers should not post anonymously or under an alias to evade the guidance given in this policy.
- Pupils and parents/carers **must not** post content online which is damaging to the school or any of its staff or pupils.
- Pupils at Three Rivers Federation should not sign up to social media sites that have an age restriction above the pupil's age.
- If inappropriate content is accessed online on school premises, it **must** be reported to a teacher.

Blocked content - (will need to discuss with the IT staff)

We need to know what is blocked currently

Attempts to circumvent the network's firewalls will result in a ban from using school computing equipment, other than with close supervision.

- Inappropriate content which is accessed on the school computers should be reported to the Headteacher so that the site can be blocked.
- Requests may be made to access erroneously blocked content by speaking to the Headteacher.
- The final decision on whether access should be granted to a site will be made by the Headteacher.

Cyber bullying

Cyber bullying is taken seriously.

- Incidents of cyber bullying will be dealt with and reported along the same chain as the Anti-Bullying Policy.
- Staff members should never respond or retaliate to cyberbullying incidents. Incidents should instead be reported as inappropriate, and support sought from senior staff member.
- Evidence from the incident should be saved, including screen prints of messages or web pages, and the time and date of the incident.
- Where the perpetrator is a current pupil or colleague, most cases can be dealt with through the school's own disciplinary procedures.
- Where the perpetrator is an adult, in nearly all cases, a senior staff member should invite the victim to a meeting to address their concerns. Where appropriate, the perpetrator will be asked to remove the offensive content.
- If the perpetrator refuses to comply, it is up to the school to decide what to do next. This could include contacting the internet service provider in question through their reporting mechanisms, if the offensive content breaches their terms and conditions.
- If the material is threatening, abusive, sexist, of a sexual nature or constitutes a hate crime, the school should consider contacting the police.
- As part of our on-going commitment to the prevention of cyber bullying, regular education and discussion about e-safety will take place as part of computing and PSHE.

Be SMART online

We encourage pupils to take a SMART approach to social media behaviour:

Safe – Do not give out personal information, or post photos of yourself to people you talk to online. Follow age restriction rules.

Meeting – Do not meet somebody you have only met online. We encourage parents/carers to speak regularly to their children about who they are talking to online.

Accepting – We advise that pupils only open emails and other forms of communication from people they already know.

Reliable – We teach pupils about the dangers of believing everything they see online.

Tell – We encourage pupils to tell a teacher, parent or carer if they see anything online that makes them feel uncomfortable.

January 2018.