Acceptable Use of ICT Policy

Lead member of staff:	L Farmer (Assistant Headteacher, Pastoral)
Legislation Status: (Statutory/Non-Statutory)	Statutory
Local Authority Model Policy or School Written Policy:	School Written Policy
Required on school website:	Yes
Revision Date:	May 2023
Date Ratified By Full Governing Body:	June 2023
Signed By Chair Of Governors: **Ms C Hardy**	C Hardy

The acceptable use of ICT, including social media agreement

Overview

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this acceptable use agreement annually.

All staff must be aware that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites. This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

1. Digital communication

- Digital communications with students (e.g. via. e-mail) should be on a professional level and only carried out using official school systems only.
- Under no circumstances should staff contact students, parents/carers or conduct any school business using personal e-mail addresses.
- School e-mail is not to be used for personal reasons. Staff must not use a personal email account or personal mobile phone to contact pupils and must not give them personal phone numbers.

2. Mobile Phones

- School mobile phones, only, should be used to contact parents, carers, or students when on school business with students off site, e.g. a school trip.
- Staff should not use personal mobile devices under any circumstances, unless with the explicit permission of the Headteacher. In such circumstances the 'caller ID' should be disabled.
- Staff should not be using personal mobile phones in school during working hours when in contact with children. Personal mobile phones must not be used by staff or visitors in public areas under any circumstances.
- Staff must never, under any circumstance, examine the contents of a student's mobile phone. The Headteacher and Designated Safeguarding Lead (DSL)/Deputy DSLs are the only staff permitted to do so.
- Students should adhere to the rules and guidelines set out in the Relationship and Behaviour Policy regarding mobile phone use in school. It is vital that all staff enforce these rules and guidelines.

- A school mobile phone only should be used on all school trips in accordance with the school's educational visits policy.
- Personal mobile phones must never be used to photograph, film or record students, either in school or with students' offsite.

3. Social Networking Sites

- Staff must not be in contact, or add as friends, any pupils and parents/carers of the school via ANY social networking sites such as Facebook, Twitter, Instagram, etc. without written permission for specific purpose from the Headteacher.
- Staff are strongly advised to ensure that when using social networking sites, personal data is kept private. Staff should use the security settings to control access to their profile.
- Students will not be allowed on social networking sites at school. Staff must not encourage students to use social networking sites at school.
- Staff should not access social networking sites on school equipment in school or at home. Staff should access sites using only personal equipment.
- Staff users should not reveal names of staff, students, parents/carers or any other member of the school community on any social networking site or blog.
- Students, parents/carers should be aware the school will investigate misuse of social networking if it impacts on the well-being of other students or stakeholders.
- If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant social networking site, and West Midlands Police, if necessary.
- Legal but harmful content will be reported using the SWGFL online reporting tool - https://swgfl.org.uk/services/report-harmful-content/report-harmful-content-button/
- Staff must promote online safety with the pupils in their care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create

4. Websites

- In lessons where Internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Staff will preview any recommended sites before use. Certain websites are automatically blocked by the school's filtering system. "Open" searches (e.g. "find images/ information on...") are discouraged when working with students who may misinterpret information.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff.
- All users must observe copyright of materials published on the Internet.
- Staff will judge which students are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the students on the internet by the member of staff setting the task. All staff are aware that if they pass

students working on the internet that they have a role in checking what is being viewed. Monitoring software such as AB tutor must be used when available.

5. Passwords

- Staff passwords or encryption keys should not be recorded on paper or in an unprotected file and should be changed at least every 3 months. Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems
- Staff must respect system security and must not disclose any password or security information. Staff must use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).

6. Use of Equipment

- Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Headteacher or the ICT Network Manager.
- No personally owned applications or software packages should be installed on to school ICT equipment;
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs.
- All staff should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.
- Staff must not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the ICT Network Manager.
- Staff understand that any hardware and software provided by their workplace for staff use can only be used by members of staff and only for educational use.
- To prevent unauthorised access to systems or personal data, staff must not leave any information system unattended without first logging out or locking my login as appropriate.

7. Data storage

- Staff must ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the General Data Protection Regulation (GDPR) and the school's data protection policy.
- Any images or videos of pupils must only be taken and/or used where there is parental consent. Any images or videos of staff must only be taken and/or used where there is staff consent.
- Staff are expected to save all data relating to their work to their laptop if they have been assigned one, or to the school's VLE
- Teachers are not permitted to use removable media such as, USB pen drives, CDs, portable drives unless permitted by the Headteacher.

- Behaviour and relationship profiles, EHCPs, assessment records, student medical information and any other data related to students or staff should not be stored on personal memory sticks but stored on an encrypted USB memory stick provided by school or on our secure VLE.
- Only take offsite information you are authorised to and only when it is necessary and required in order to fulfil your role. If you are unsure speak to a member of SLT.
- Staff must respect copyright and intellectual property rights and adhere to the terms and condition of all licence agreements relating to software and learning resources.

8. Remote Learning

- Microsoft Outlook and Microsoft Teams are the school's chosen methods for remote learning and virtual meetings when they are required.
- Remote learning may be used at the direction of SLT. For remote learning all staff will use a mixture of asynchronous and synchronous methods for teaching.
- For synchronous lessons pupils will not be required to enable their cameras and will remain muted, unless they are in the Sixth Form.
- Teachers are not required to enable their cameras whilst delivering synchronous lessons.
- When delivering synchronously the 'lobby' function in Teams must be used to control access to the lesson. Only members of the school community may access Microsoft Teams.
- When creating 'classes' within MS Teams it is vital that Heads of Department are included in all classes for their department. This will enable leaders to provide effective support and guidance when required.
- All lessons on MS Teams must be delivered asynchronously if there are less than three pupils in the Teams 'class'. Sixth Form lessons may be delivered with less than three pupils but must be auditable.
- There may be circumstances when staff may need to meet with pupils virtually using Microsoft Teams, e.g. wellbeing checks with pupils, EHCP reviews. Any one-to-one sessions, for example pastoral care meetings, should be risk assessed and approved by the school's leadership team.
- Meetings must only take place during normal school hours, except for online tuition organised by the school.
- If Microsoft Teams is used to meet with individual pupils there must be two members of staff present in the virtual meeting. The parents of pupils must provide consent before any meeting takes place and should be encouraged to attend the meeting.
- Digital communications with students (e.g. via. e-mail) should be on a professional level and only carried out using official school systems.
- Private systems (e.g. personal Google, YouTube Channel, Microsoft emails or personal usernames) should never be used and personal staff mobile numbers should not be given out to students.

- All one-to-one tutoring or messaging, unless this is pre-approved by the Headteacher and auditable, should be avoided. Any communication with pupils must be copied into the appropriate line manager.
- Ensure that all resources created for remote learning are private and therefore not available to the public by checking privacy settings within the platform used.
- When creating virtual resources staff are bound by the school's expectations regarding professional conduct.
- If a member of staff creates a virtual resource this must be uploaded to the school's VLE so that the resource can be reviewed if necessary. This should be monitored by Heads of Department and senior leaders.
- If a member of staff creates a video for students to use they must not include their own image or anything that is linked to their personal identity. This is it to ensure that it is not used inappropriately by pupils accessing the video.
- If an external visitor attends a 'live lesson' virtually the school's arrangements for visits and hosting a visit should be adhered to.
- Any incidents of concern regarding pupil's online safety must be reported to the DSL or a deputy via CPOMS as soon as possible.
- The following guidelines are based on the following DfE guidance: https://www.gov.uk/government/publications/providing-remote-education-guidance-for-schools

9. Safeguarding

- Staff must report all incidents of concern regarding pupil's online safety to the DSL or Deputy DSL as soon as possible. Staff must report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the DSL Andy Oliver or Deputy DSLs Jacqui Peterkin.
- All synchronous lessons are recorded for safeguarding reasons. If a lesson is delivered outside of school it must be recorded on the school device. It is the teacher's responsibility to ensure that these lessons are recorded.
- If staff have any queries or questions regarding safe and professional practice online either at the school or offsite, these must be raised with the DSL, or Headteacher.
- If staff have any concerns regarding the conduct of a member of staff online, they must be raised immediately with the Headteacher. If this concern relates to the Headteacher this must be raised with the Chair of Governors.
- Staff must understand that their use of the school's information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- Note that the procedures and policies outlined in this policy may be reviewed or changed at any time. Staff will be informed of any important changes. If staff have any queries or questions regarding safe and professional practice online either at the school or offsite, these must be raised with the DSL or Deputy DSL, or Headteacher.