STAFF USE OF ICT POLICY

Reviewed:	May 2024
Review date:	May 2025
Person responsible for policy:	DCC

STAFF USE OF ICT POLICY

Policy Contents

This Policy includes:

- Use of Internet and Email
- Use of Social Media
- Monitoring of usage of Internet, Email and Social Media
- Use of the School hardware, network and associated online storage locations.

A separate policy (Student Use of ICT Policy) applies to student use of ICT and can be found within the E-Safety Policy.

This policy should be read in conjunction with the Schools Data Protection Policy, Data Transfer Security Policy and Data Retention Policies. Droitwich Spa High School and Sixth Form Centre takes its responsibilities as a data controller and data processor seriously and is committed to using any personal data collected and held in accordance with the law. The schools policies in regard to personal data as well as the relevant privacy notices in relation to personal data are available on the School's Portal or web site and employees are expected to read and be familiar with them.

The School's Data Protection Officer is the *Governance Manager* who can be contacted at Droitwich Spa High School and Sixth Form Centre, Briar Mill, Droitwich, WR9 0AA or by email at privacy@droitwichspahigh.worcs.sch.uk

Additionally, there is also an acceptable use policy for staff and students, intended as a quick reference document displayed in ICT classrooms.

1. Scope of Policy

This policy applies to all people who are employed by the school. They are collectively referred to as staff in this policy.

Third parties (not including students, who have a separate policy) who have access to our electronic communication systems and equipment are also required to comply with this policy. It will be the responsibility of the member of staff who grants a third party access to make sure that they are informed of the obligations that come with use of the facilities.

This policy applies to the use of:

- all internet, intranet and email facilities, multi-user computers, workstations, network storage locations (both physical locations and storage allocated to the organisations via cloud storage, micro-computers and any networks connecting them provided by the School;
- all hardware owned, leased, rented or otherwise provided the School.
- all hardware owned, leased, rented or otherwise provided by a member of staff and connected to or otherwise accessing our networks or other facilities.

Policy relating to the expectations of staff with regards to the e-safety of students is contained in the Safeguarding Policy.

2. Hardware not owned or leased by the School

Staff must not connect hardware that is not owned or leased by the School to physical network data sockets. Connecting hardware that is not owned or leased by the school to projectors and wireless networks is permitted.

3. Implementation of the Policy

The Headteacher has overall responsibility for the effective operation of this policy, but has delegated day to day responsibility for its operation to the member of the Senior Leadership Team responsible for ICT Systems Management. Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risk also lies with the member of the Senior Leadership Team responsible for ICT Systems Management. Questions regarding the content or application of this policy should be directed to the member of the Senior Leadership Team responsible for ICT Systems Management or the Headteacher.

All Heads of House and members of the Senior Leadership Team should ensure that all staff understand the standards of behaviour expected of them, if necessary enforcing this policy by taking action when behaviour falls below its requirements.

Failure to follow the Policy

Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details so far as this is consistent with the right of an individual to private and family life.

Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

4. Use of Internet and Email

4.1 Unauthorised Use

Within this policy "inappropriate communication" includes any form of communication which is against the best interests of the School, or which could bring the School into disrepute or subject the School to any legal liability.

The facilities must be used in a responsible manner. Staff must not interfere with the work of others or the system itself. In particular, they must not create, transmit or cause to be transmitted:

- material which is designed, or likely to cause annoyance, inconvenience, needless anxiety or offence, and you must not create, transmit or cause to be transmitted offensive, obscene or indecent material, unless in the proper course of your duties;
- material about any individual, organisation or product without having taken reasonable steps to verify its accuracy;
- knowingly defamatory material, including opinions expressed about any individual, organisation or product;
- material whereby the copyright of another person is knowingly infringed;
- material that is unlawful;
- material which is vulgar, obscene or contains sexually or racially explicit language or material;
- racist, sexist, homophobic, transphobic, extremist, discriminatory (including against those with disabilities) or harassing material or language;
- any message internally or externally which is abusive, humiliating, hostile or intimidating;

In addition staff must not:

- gain deliberate unauthorised access to facilities or services accessible via local or national networks or the world wide web;
- gain unauthorised access to, or violate the privacy of, other people's files, email account, corrupt or destroy other people's data or disrupt the work of other people;
- disclose passwords to third parties without the consent of the School;
- disclose usernames and passwords to other members of staff or students without the consent of the school.
- permit anyone to use any facilities using personal login details, even if login details are not disclosed (i.e. logging on to a system and then permitting someone else to use that login);
- transmit by email any confidential information of the School including information about any pupils, parents, or staff of the School, other than in the normal course of duties;
- join any mailing groups or lists that could result in receiving of messages that would be in breach of any part of the rest of this policy;
- send any message purporting to be someone else;
- play computer games either networked or otherwise, unless the games were intended for educational use;
- transmit or cause to be transmitted any repetitive emails to bulk recipients (spamming) save in the course of your duties;
- respond to, or open any attachment received by, an unknown sender, especially those requesting personal or sensitive data (phishing) and report it immediately to the ICT Support Team;
- circumvent or attempt to circumvent any anti-virus, malware and any other security software;
- store excessive or unnecessary email communication for an unnecessary period of time.

Inappropriate communication includes all of the above, but the list is not exhaustive.

4.2 Authorised Use

The email system is available for communication on matters directly concerned with the business of the School. Whilst using the internet or email staff must:

- observe this policy at all times and note the disciplinary consequences of non-compliance, which in the case of a gross breach or repeated breach of the policy may lead to dismissal;
- ensure that the School's standard email sign-off and disclaimer for all messages;
- produce and write email with the care normally given to any form of written communication;
- appreciate that email is relatively insecure and consider security needs and confidentiality requirements before any transmission;
- consider the contents of emails received and the intentions of the original sender when deciding whether to forward to other recipients, either internal or external;
- not knowingly disclose any unique password to any unauthorised person and make all reasonable efforts to ensure that the confidentiality of any such password is maintained;
- not access or share an email mailbox of another member of staff without the permission of the Headteacher and where possible the prior agreement of all members of staff involved. (Further clarification of accessing staff mailboxes in the event of absence is clarified in section 3)

If staff are in doubt about sending any confidential material, they should consider sending the information in another form. Email messages can be used as evidence in court proceedings. It is possible to enter into a legally binding contract using email.

4.3 Use of the Internet and Email for Personal Purposes

Excessive use of email and Internet facilities for personal purposes is not permitted. However, the School acknowledges that limited personal use may occur from time to time. Any such use must be in accordance with this policy and must not disrupt your duties. You are not permitted to make personal purchases. Only those authorised to do so in the Finance Team may make purchases for school use (as stipulated in the Finance Policy.) Abuse or excessive use of the email and/or internet will be dealt with through the disciplinary procedure.

5 Use of Social Media

5.1 Scope of the policy

The policy applies to the use of social networking sites for School and for personal use, whether they are being used during school hours, or otherwise, and whether they are being accessed using the School's equipment, or personal equipment.

A social networking site is any website which enables its users to create profiles, form relationships and share information with other users. It also includes sites which have online discussion forums, chat-rooms, media posting sites, blogs and any other social space online. It includes but is not limited to, sites such as Facebook, Twitter, Instagram, Snapchat, Pintrest, Reddit, Linkedin and Dating websites.

5.2 Responsible use of social media

Staff must also be aware of the particular risks to internet security that social media presents. In order to comply with the existing School policy Use of Internet and Email, staff must take any extra measures necessary not allow any of their actions on social media sites to create vulnerability to any School systems.

Staff must:

- ensure that wherever possible their privacy settings on social media sites are set so that pupils cannot access information relating to their personal lives;
- obtain the prior written approval of the Headteacher, to the wording of any personal profile which a member of staff intends to create where the School is named or mentioned on a social networking site;
- seek approval from the Headteacher before they speak about or make any comments on behalf of the School on the internet or through any social networking site;
- report to the Headteacher or other member of the Senior Leadership Team immediately if they see any information on the internet or on social networking sites that disparages or reflects poorly on the School;
- immediately remove any internet postings which are deemed by the School to constitute a breach of this or any other School policy;
- weigh whether a particular posting puts their effectiveness as a member of staff at risk;
- post only what they want the world to see.

Staff must not:

- provide references for other individuals, on social or professional networking sites, as such references whether positive or negative can be attributed to the School and create legal liability for both the author of the reference and the School;
- post or publish on the internet or on any social networking site, any reference to the School, your colleagues, parents or pupils;
- use commentary deemed to be defamatory, obscene, proprietary, politically or religiously extreme or libellous. Staff must exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterisations;
- discuss pupils or colleagues or publicly criticise the School or staff;
- post images that include pupils;
- initiate friendships with current or future pupils on any personal social network sites;
- accept current or future pupils as friends on any such sites; staff must decline any pupil-initiated friend requests;
- Accept friend requests/follows or any other connection from current students, or ex-students who are under the age of 18.

- use social networking sites as part of the educational process e.g. as a way of reminding pupils about essay titles and deadlines, except where a non-personal account has been set up with the sole purpose of doing so.

5.3 Personal use of social media

Personal use of social media is never permitted by means of School computers, networks and other ICT resources and communications systems.

Staff must not use their School email address for any personal use of social media.

5.4 Social media and the recruitment process

The School use internet searches to perform due diligence on candidates in the course of recruitment. Where we do this, we will act in accordance with our data protection and equal opportunities obligations.

6 Monitoring of use of the Internet, Email and Social Networking

The contents of our IT resources and communications systems are the School's property. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

The School will endeavour to respect your right to privacy, however we reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies for the purpose of:

- establishing the existence of facts;
- ascertaining compliance with regulatory or self-regulatory policies, practices or procedures;
- ascertaining or demonstrating standards which are expected to be achieved by persons using the system (eg. quality control);
- preventing and detecting crime;
- investigating or detecting unauthorised use of the system, as set out in this policy;
- ensuring the effective operation of the system;
- checking that communications are relevant to the work of the School.

The School may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

The School will endeavour not to read personal emails save where necessary for the reasons set out above.

If a member of staff is absent from work, his/her mailbox may be checked for the purpose of checking that communications are relevant to the work of the School and ensuring that the School responds promptly to pupils, parents and contacts. This access may be granted to the relevant Head of House by submitting a request to the Headteacher. This access will be time bound and monitored accordingly.

Record Keeping

We will comply with the provisions of the Data Protection Act 1998/General Data Protection Regulation (GDPR) 2018 and abide by our Data Protection Policy.

Hard copy emails may be retained where appropriate. Hard copies of emails can be used as evidence in disciplinary proceedings.

7 Use of the School Hardware, Network and associated online storage locations

7.1 Scope of the policy

The policy applies to the use of ICT hardware, including laptops, printers and electronic devices, as well as any network or cloud storage locations or online services, either owned, managed or subscribed to by the school for the purposes of education and its effective administration.

Whilst some personal use of staff laptops is expected, staff must comply with the following conditions in order to ensure the safe, efficient and acceptable use of school hardware. This is in order to avoid damage to either the device independently or the wider school network, as well as enabling the effective allocation of storage to all users.

Staff must:

- make every effort to ensure the safe operation, security, transport and storage of ICT equipment owned by the school, both on and off site;
- ensure all ICT issues, both operational and technical, are reported via the correct channels to the ICT Support Team;
- consult the ICT Support Team regarding the installation of specific software not installed as part of the generic school image;
- ensure laptops, workstations and electronic communication devices are locked when left unattended;
- ensure work is saved to their allocated user area so that effective backup and monitoring may take place.

Staff must not:

- allow any non-school employee to use their staff laptop for business or recreational use;
- install, or attempt to install non-school related software including games or applications;
- store personal or non-work related files to their user area;
- use or depend on school hardware and systems for personal or business based documentation (e.g exam marking/moderation). It is the member of staff's responsibility to secure and backup data of this nature;
- store excessive or unnecessary files to their staff laptop C: drive;
- attempt to repair, modify, deface or disassemble any ICT equipment;
- allow students to use staff laptops or desktops, or provide login credentials to achieve the former.

Droitwich Spa High School and Sixth Form Centre takes its responsibilities as a data controller and data processor seriously and are committed to using any personal data collected and held in accordance with the law. The schools policies, privacy notices and forms in relation to personal data are available for you to view on our web site at www.droitwichspahigh.worcs.sch.uk or by using the https://website.droitwichspahigh.worcs.sch.uk/index.php/communications/information-management-and-data-protection/
The School's Data Protection Officer can be contacted at Droitwich Spa High School and Sixth Form Centre, Briar Mill, Droitwich, WR9 0AA or by email at privacy@droitwichspahigh.worcs.sch.uk