Acceptable Use of IT Policy

Reference: DPO

Policy date	**New version July 2023**	**Statutory Policy - Yes**
Strategic Board Approval	**July 2023**	
Reviewed and Updated	**First version**	
Next Review Date	**July 2024**	**Annual**
Author	**DPO/NS**	**www.acexcellence.co.uk**

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users have an entitlement to safe internet access at all times.

Misuse of IT and communication systems can damage the organisation and our reputation. Breach of this policy may be dealt with under our Disciplinary Policy and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

This policy does not form part of any contract of employment and may be amended at any time.

Who does this policy apply to?

This policy applies to all employees, consultants, self-employed contractors, agency workers and volunteers. It also applies to anyone who has access to our IT and communications systems.

Who is responsible for this policy?

The Board of Directors has overall responsibility for the effective operation of this policy. The Board of Directors has delegated responsibility for overseeing its implementation to the People Team. Suggestions for changes to this policy should be reported to the People Team.

Any questions you may have about the day to day application of this policy should be referred to (your line manager or People Department) in the first instance.

This policy is reviewed annually by DPO.

This Acceptable Use Policy is intended to ensure that:

• Staff, governors and anyone using the school systems will be responsible users and stay safe whilst using the internet and other communications technologies for educational, personal and recreational use.

• School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

• Staff are protected from potential risk in their use of IT in their everyday work, including remote learning. The school will endeavour to ensure that all staff and visitors will have good access to IT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and visitors to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users including students. I recognise the value of the use of IT for enhancing learning and will ensure that students receive opportunities to gain from the use of IT. I will, wherever possible, educate the students in my care in the safe use of IT and embed e-safety in my work with the students.

For my professional and personal safety:

• I understand that the school may monitor my use of the ICT systems, email, file storage and other digital communications. Any monitoring will be carried out in line with *The Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 and the Data Protection legislation.*

• I understand that the rules set out in this agreement also apply to use of school IT systems (for example iPads, email etc) when out of school and during any remote learning sessions that may take place.

• I understand that the school IT systems and equipment are primarily for educational use. My personal or recreational use should be kept to a minimum within the policies and rules set down by the school and should not interfere with work commitments. I understand that any personal use of the systems may be monitored and where breaches of the policy are found, action may be taken under our disciplinary policy.

• I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

• I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the DPO.

I will be professional in my communications and actions when using school IT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I will demonstrate and appreciate that others may have different opinions.

- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images temporarily, if the school's policies expressly permit me to do so and if the equipment is password protection/pin coded. Images of children obtained through the school must never be retained on personal devices, after the images have been transferred onto school

equipment/systems.

- Where images are published (eg on the school website) it will not be possible to identify those who are featured by full their name, or other personal information.

- I will only use chat and social networking sites in school in accordance with the school's policies.

- I will not engage in any on-line activity that may compromise my professional responsibilities or bring the school into disrepute.

- I will only communicate with students and parents / carers using official school systems. Any such communication will be professional in tone and manner.

- I will not use my school email address for personal matters.

- I understand if the data on any device is breached, I will report it to the Senior Leadership Team and our Data Protection Officer, through the school's Data Protection Link Officer at annette.henry@devon.gov.uk

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- Where I am expressly permitted to use my personal equipment to access the school's emails or systems (such as through my iPad, tablet, laptop, personal computer or mobile phone), I will ensure the security of that data by following the school's policies and security guides. I will also follow any additional rules set by the school about such use.

- I understand that personal information relating to pupils/students or staff cannot be stored on any personal equipment, unless in rare and expressly permitted circumstances. In such cases, the personal equipment must be encrypted or otherwise suitably protected with a pin code, password, thumb print etc.

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

- I will take care of the content of all emails as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. You do not have any control over whether an email may be forwarded by the recipient. I will avoid saying anything which could cause offence or embarrassment if it was forwarded to any third party.

- I understand that email messages are required to be disclosed in legal proceedings. Deletion from my inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

- I will not use my own personal email address to send or receive emails for the purposes of the organisation.

- If I receive an email in error, I will notify the sender.

- I will ensure that any data that I work on locally on my iPad is regularly saved into a secure school network folder and ensure it is regularly backed up and appropriately secured.

- I will not try to upload, download or access any materials which are illegal (eg child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials. Anyone who is has concerns about inappropriate material should inform their line manager or the People Team Lead.

- I will not attempt to transfer large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.

- I will not attempt to gain access to restricted areas of the network, or to any password protected information, except as authorised in the proper performance of my duties.

- I will not disable or cause any damage to school equipment or the equipment belonging to others.

- I understand that in line with UK GDPR there are several associated policies which outline the requirement that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority. These policies are:

    - Privacy Notice for Parents/Students
    - Privacy Notice for Employees
    - Privacy Notice for Members, Directors and Local Governors
    - Data Protection Policy

- I understand that when engaging the services of an App or cloud-based service that is processing personal data that, with the engagement of the DPO Link/DPO, I ensure that a Data Processing Impact Assessment is conducted to evaluate and assess risks related to the processing of the personal data.

- I understand that the use of USB sticks to transfer personal and confidential data is prohibited unless the storage device has been encrypted or pseudonymisation has been carried out by IT Support.

- I understand that when I am using a personal device (PC, laptop or tablet) to conduct school related work, I will:

    - Log out when I leave my device, especially if I share the device with a family member
    - Turn off my microphone when I finish a live session – if I am delivering remote learning
    - Ensure my device is password protected
    - Not save any school data on my personal device and check my download folder does not hold any school data
    - Not ignore the Windows or Mac upgrades as they have important security patches
    - Ensure virus protection on my PC or laptop is up to date

- I will send personal, sensitive information via Egress (secure email) when required to do so.

- I understand that I must be particularly vigilant when using IT equipment outside of the workplace and take appropriate precautions as we required to protect against viruses or compromising system security. The system contains information which is confidential and subject to data protection legislation. This information must be treated with extreme care and in accordance with our Data Protection Policy.

Prohibited Use of our Systems

- Misuse or excessive use of our IT and communication systems will be dealt with your our Disciplinary Policy. Misuse of the internet can in some circumstances be a criminal offence. In particular, it will usually amount to gross misconduct to misuse our systems by participating in online gambling, forwarding chain letters, by creating, viewing, accessing or downloading any of the following material (this list is not exhaustive):
  (a) Pornographic material (including writing, pictures, films and video clips of a sexually explicit or arousing nature)
  (b) Offensive, obscene or criminal material which is liable to cause embarrassment to the organisation or cause detriment to our reputation.
  (c) A false or defamatory statement about any person or organisation
  (d) Material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Diversity and Inclusion Policy or Bullying Policy)
  (e) Confidential information about the organisation, our staff or pupils (except as authorised in the proper performance of your duties)
  (f) Unathorised software
  (g) Any other statement which is likely to create criminal liability (for you or the organisation)
  (h) Music, videos or other material in breach of copyright.

  Any such action will be treated very seriously and is likely to result in summary dismissal.

  Where evidence of misuse is found, we may undertake a more detailed investigation in accordance with our disciplinary policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Policy. If necessary, such

information may be handed in to the police in connection with a criminal investigation.