

STOW-on-the-WOLD PRIMARY SCHOOL

heart hand mind

Acceptable IT Use Agreement Staff and Volunteers Policy



Approved by: Full Governing Body

Date: 5th February 2024

Last reviewed on: 1st February 2024

Signature: T. A. Bartlett

Next review due by: 1st February 2025

Chair of Governors

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up 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 should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school/academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

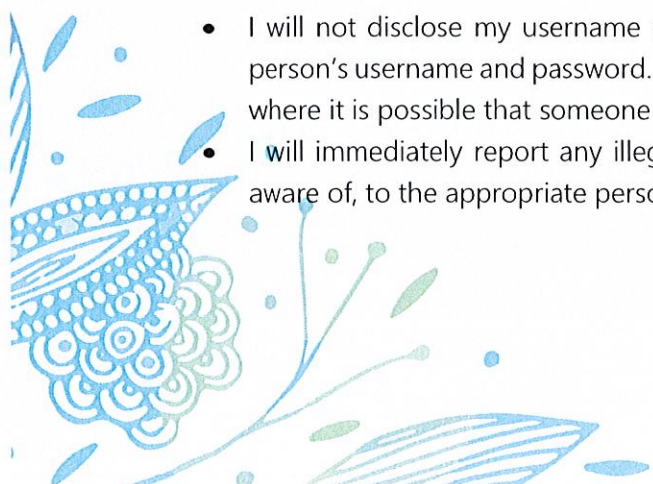
The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *students/pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that *students/pupils* receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use
- 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

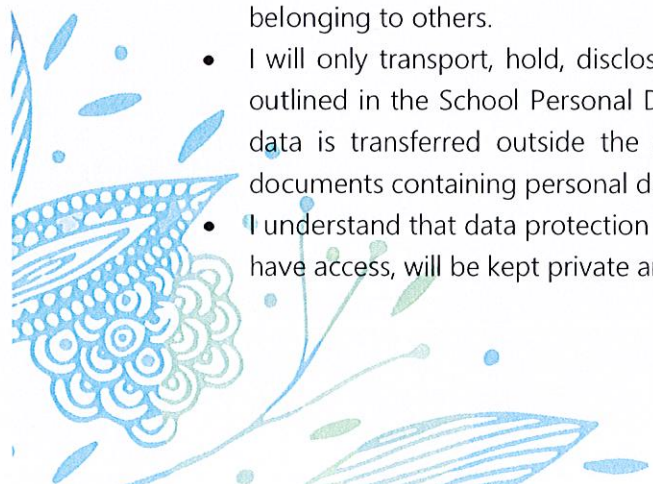


I will be professional in my communications and actions when using the school systems:

- 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 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, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school/academy*:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school/academy ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school/academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist 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.
- I will not try (unless I have permission) to make 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 on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school/academy policies
- I will not disable or cause any damage to school/academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires 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/academy policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school/academy*:

- I understand that this acceptable use policy applies not only to my work and use of school/academy digital technology equipment in school, but also applies to my use of school/academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

I have read the appendix below relating to remote learning, virtual lessons and live streaming.

Staff/Volunteer Name:

Signed:

Date:

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2020. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.



Appendix One Remote education, virtual lessons and live streaming

Delivering remote education safely, keeping children safe online is Annex C provides schools and colleges with information on what they should be doing to protect their pupils online.

At Stow Primary School we have :

- Reviewed and amended our online safety and acceptable use policies to reflect the current situation
- ensured that all relevant staff have been briefed and understand the policies and the standards of conduct expected of them
- have clearly defined operating times for virtual learning
- considered the impact that virtual learning may have on children and their parents/carers/siblings
- carefully considered the context of our own setting and appropriate use of live lessons; considered whether other options might be more suitable in some contexts – for example, using audio only, pre-recorded lessons or existing online resources
- been made aware of the virtual learning timetable and ensure that the Head has a capacity to drop in, unscheduled, on a range of lessons
- take into account any advice published by the Department for Education, local authority, multi-academy trust or their online safety/monitoring software provider

Staff should:

- adhere to their establishment's policy
- be fully dressed
- ensure that a senior member of staff is aware that the live lesson/meeting is taking place and for what purpose
- only record a lesson or online meeting with a pupil where this has been agreed with the headteacher and the pupil and their parent/carer have given explicit written consent to do so

Adults should not:

- contact pupils outside the operating times defined by the headteacher
- take or record images of pupils for their personal use
- record virtual lessons or meetings using personal equipment (unless agreed and risk assessed by HT)
- engage online while children are in a state of undress or semi-undress

In some cases, staff may need to speak to children one-on-one, for example teaching assistants might be providing extra support to children with SEND. Where this is the case, staff should ensure that parents are aware, and invited to, any one-to-one interactions with pupils and that those interactions are necessary (for example, for teaching assistants supporting SEND children). The HT should also be aware and have the option to join. Staff should also be clear about expectations around behaviour, for example, a 'classroom standard' of behaviour is expected from all participants.

For further advice and information, schools should familiarise themselves with guidance from the Department for Education.

Support on delivering online remote education safely is available from:

- safe remote learning, published by SWGfL
- online safety and safeguarding, published by LGfL, which covers safe remote learning
- the National Cyber Security Centre, which includes which video conference service is right for you and using video conferencing services securely
- safeguarding and remote education during coronavirus (COVID-19)
- annex C of keeping children safe in education, see below

Annex C: Online safety

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

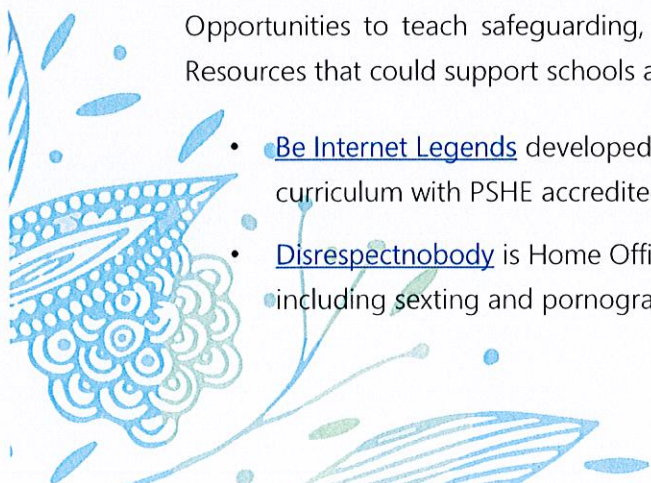
The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Education

Opportunities to teach safeguarding, including online safety, are discussed at paragraph 88-90. Resources that could support schools and colleges include:

- [Be Internet Legends](#) developed by Parent Zone and Google is a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils
- [Disrespectnobody](#) is Home Office advice and includes resources on healthy relationships, including sexting and pornography



- [Education for a connected world framework](#) from the UK Council for Internet Safety supports the development of the curriculum and is of particular relevance to RSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond (covering early years through to age 18) and to be central to a whole school or college approach to safeguarding and online safety.
- [PSHE association](#) provides guidance to schools on developing their PSHE curriculum
- [Teaching online safety in school](#) is departmental guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements
- [Thinkuknow](#) is the National Crime Agency/CEOPs education programme with age specific resources
- [UK Safer Internet Centre](#) developed guidance and resources that can help with the teaching of the online safety component of the Computing Curriculum.

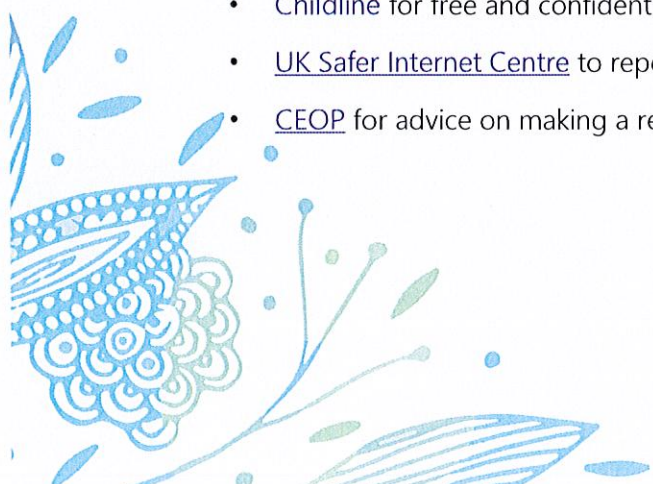
Education at home

Where children are being asked to learn online at home the department has provided advice to support schools and colleges do so safely: [safeguarding-in-schools-collegesand-other-providers](#) and [safeguarding-and-remote-education](#)

- [Case studies](#) on remote education practice are available for schools to learn from each other
- [Departmental guidance on safeguarding and remote education](#) including planning remote education strategies and teaching remotely
- [London Grid for Learning](#) guidance, including platform specific advice
- [National cyber security centre](#) guidance on choosing, configuring and deploying video conferencing
- [National cyber security centre](#) guidance on how to set up and use video conferencing
- [UK Safer Internet Centre](#) guidance on safe remote learning

Support for children at home

- Childline for free and confidential advice
- [UK Safer Internet Centre](#) to report and remove harmful online content
- [CEOP](#) for advice on making a report about online abuse



Parental support

- [Childnet](#) offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- [Commonsensemedia](#) provide independent reviews, age ratings, & other information about all types of media for children and their parents
- [Government advice](#) about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- [Government advice](#) about security and privacy settings, blocking unsuitable content, and parental controls
- [Internet Matters](#) provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- [Let's Talk About It](#) provides advice for parents and carers to keep children safe from online radicalisation
- [London Grid for Learning](#) provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- [Lucy Faithfull Foundation StopItNow](#) resource can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- [National Crime Agency/CEOP Thinkuknow](#) provides support for parents and carers to keep their children safe online
- [Net-aware](#) provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- [Parentzone](#) provides help for parents and carers on how to keep their children safe online
- [Parent info](#) from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations

[UK Safer Internet Centre](#) provide tips, advice, guides and other resources to help keep children safe online

