# E-Safety Policy

| |
|---|
| Policy & Procedure Number: 69 |
| Date of Board of Governors Review: Autumn 2019 |
| Next Review Due: Autumn 2022 |
| School Link: Miss Leanne Healey |
| Revision Number: v2 |

## 1 Introduction

**1.1** ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

1.2 Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the Internet technologies children and young people are using both inside and outside of the classroom include:

- Websites;
- Learning Platforms and Virtual Learning Environments;
- Email and Instant Messaging;
- Chat Rooms and Social Networking;
- Blogs and Wikis;
- Podcasting;
- Video Broadcasting;
- Music Downloading;
- Gaming;
- Mobile / Smart phones with text, video and/ or web functionality;
- Other mobile devices with web functionality.

**1.3** Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

**1.4** We understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

**1.5** Both this policy and the **Acceptable Use Agreement** (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.) and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc…).

**1.6** This policy should be read alongside the following policies: Code of Conduct; Safe Working Practices; Social Media Policy; Information & Communication Systems Policy and Mobile Phone Policy.

## 2 Roles and Responsibilities

**2.1** As e-safety is an important aspect of strategic leadership within the school, the Principal and Governors have ultimate responsibility to ensure that the policy and practices are embedded

and monitored. For the purposes of this document the following staff are referenced throughout:

| | |
|---|---|
| Principal | Simon Corner |
| Vice Principal/DSL | Claire Ward |
| DDSLs | Nicola Harrison; Judith Bairstow; Matthew Deeney; Adam Mitchell |
| ICT Network Manager | Peter Waring |

**2.2** All members of the school community have been made aware of who holds these posts. It is the role of the Principal to keep abreast of current issues and guidance through organisations such as Halton LA, CEOP (Child Exploitation and Online Protection) and Childnet.

**2.3** Senior Management and Governors are updated by the Principal and all Governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice. This policy, supported by the school's **Acceptable Use Agreement** (for staff, governors, visitors), is to protect the interests and safety of the whole school community.

## 3 Child Protection/Safeguarding Designated Person

**3.1** The Child Protection/Safeguarding Designated Person should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data;
- Access to illegal/inappropriate materials;
- Inappropriate on-line contact with adults/strangers;
- Youth produced Sexual Imagery;
- Potential or actual incidents of grooming;
- Cyber-bullying;
- Terrorism and extremism material.

## 4. Online Safety

**4.1** New staff receive information on the school's Acceptable use Agreement as part of their induction. All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.

**4.2** All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas. This is also taught through the school's SMSC programme as well as through pastoral messages and assemblies.

**4.3** In teaching students about e-safety, the school uses the DFE's guidance on how to stay safe online: *Teaching online safety in school* (June 2019) which has a focus on the following areas:

- Knowledge and behaviours;
- Harms and risks;
- Navigating the Internet and managing information;

- How to stay safe online;
- Well-being.

**4.4** The teaching of online safety also makes reference to Annex C (Online Safety) from 'Keeping Children Safe in Education' (2019) given that the use of technology has become a significant component of many safeguarding issues.

**4.5** The school's website has a dedicated page for Parents/Carers with advice on how to keep children safe online. This is regularly updated with advice to parents about Internet safety.

## 5 Safeguarding/Prevent

**5.1** Under duties imposed within the Prevent Duty Guidance 2015 as part of the Counter-Terrorism and Security Act 2015, Wade Deacon High School will ensure that situations are suitably risk assessed, that they will work in partnership with other agencies, that all staff are suitably trained and that IT policies will ensure that children and young people are safe from terrorist and extremist material when accessing the Internet in school.

**5.2** The School Lead (Single Point for Contact) for Prevent is: Nicola Harrison. The SPOC will link with other relevant agencies (including the Police) to ensure that vulnerable people are appropriately supported and risk assessed, and that staff and Governors are trained to an appropriate level to ensure they are able to recognise any concerns. The specific Roles and Responsibilities of this Single Point of Contact (SPOC) are defined in the school's Child Protection & Safeguarding Policy.

6 Password Security

**6.1** Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. Staff are regularly reminded of the need for password security. Staff are required to set their own password that meets the security requirements set out by the ICT team. Staff must regularly change passwords and ensure they are not shared.

**6.2** If staff believe their password may have been compromised or someone else has become aware of their password they must report this to ICT Support.

**6.3** Staff are made aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform.

**6.4** All users must make sure that workstations are not left unattended and are locked.

**6.5** In school, all ICT password policies are the responsibility of the System Manager and all staff are expected to comply with the policies at all times.

## 7 Data and Security

**7.1** The accessing and appropriate use of school data is something that the school takes very seriously. The school follows the Information Commissioners Office (ICO) guidelines:

- Staff are made aware of their responsibility when accessing school data.

- The Level of access is determined by either the Principal and / or the ICT Network Manager.
- Confidential or sensitive data taken off the school premises must be encrypted.
- Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any confidential or sensitive data without the express permissions of the Principal.
- Only software properly purchased and / or approved by ICT Support may be used on the school's hardware. It is the responsibility of the user to ensure that ICT Support is fully consulted if they wish to install additional software on their laptop. It is also the responsibility of the user to ensure that any licensing issues are addressed promptly.
- It is policy to store data on a network drive which is backed up each day. It is the responsibility of each individual user to ensure that data not stored on the network is backed up regularly. The School does not take responsibility for data not in the backup plan being lost, deleted stolen etc.
- Personal devices (Laptops, Mobile Phones etc…) are not permitted to be used on the system, or connected to the wireless infrastructure without the express permissions of the Principal and / or ICT Network Manager.
- The school does not guarantee the security of any information users may enter while making permitted personal use of a school computer. The school disclaims all liability that may arise from loss or harm suffered by a user as a result of that information being disclosed to or obtained by any other person and then being further disclosed or being used so as to cause loss to the user. The school disclaims all liability for such losses and any employee using a school computer for permitted private purposes does so on the basis of having agreed this disclaimer of liability.
- Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is neither the school's responsibility nor the system manager's to install or maintain virus protection on personal systems.
- If there are any issues related to viruses or anti-virus software, the ICT Network Manager should be informed.

## 8 Managing the Internet

**8.1** The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the Internet is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

**8.2** All users must observe software copyright at all times. It is illegal to copy or distribute school software, non-licensed software or illegal software. All users must observe copyright of materials from electronic resources.

**8.3** Staff will preview any recommended sites before use. Raw image searches are discouraged when working with pupils. If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

## 9 Infrastructure

**9.1** School Internet access is controlled through the NetSweeper web filtering software with a bought in whitelist solution.

**9.2** Wade Deacon High School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 2018/GDPR, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

**9.3** The school ensures children are safe from terrorist and extremist material when accessing the Internet in school, including by establishing appropriate levels of filtering in accordance with the Prevent Duty Guidance 2015.

**9.4** Staff are aware that school Internet activity can be monitored and explored further if required. Intrusions into the privacy of employees must be proportionate to the purpose of the monitoring.

**9.5** The school uses SMART Sync management control tools for controlling and monitoring workstations. If staff discover an unsuitable site, the incident must be reported immediately to the System manager or e-safety co-ordinator.

**9.6** It is the responsibility of the school, by delegation to the ICT Network Manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines.

**9.7** Staff are not permitted to download programs on school based technologies without seeking prior permission from ICT Support.

## 10 Managing email

**10.1** The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international.

**10.2** The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed. It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary, email histories can be traced. This should be the account that is used for all school business. Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.

**10.3** Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper. Staff sending emails to external organisations, parents or pupils are advised to cc. their Line Manager. The forwarding of chain emails is not permitted in school. All email users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication.

**10.4** Staff must inform either their line manager or System Manager if they receive an offensive email.

**10.5** The School will assist the relevant authorities in taking action against any employee who commits an unlawful act whilst using the School's computer facilities. The School will report criminal activity to the Police.

**10.6** Personal or business emails, whether created or stored on School equipment, constitute a School record and as such are deemed to be property of the School.

**10.7** Emails from unknown sources or which may appear suspicious must not be opened. Software received via email must not be installed. You must consult ICT Support for advice if you receive software via email or email from an unknown source or which is otherwise suspicious.

**10.8** Emails are formal documents and must not contain remarks that might be potentially embarrassing to the School, its employees or the general public.

## 11 Managing other Web 2 technologies

**11.1** Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism.

**11.2** At present, the school allows access to social networking sites for Staff within school; this allows for better connectivity with a range of e-learning technologies.

**11.3** School staff with social networking profiles should ensure that they set the privacy levels on their accounts to the maximum i.e. only people on their 'friends or trusted' lists should be able to view their pictures / private information.

**11.4** The school specifies the following guidelines should a message from a student be received:

- Do not reply to the message. Replying to a message allows the recipient to view your profile in its entirety. This is also a way to circumvent the privacy settings on accounts.

- Inform the school's safeguarding lead at the earliest opportunity and advise them of the full details of the incident. The relevant Facebook communication should be made available to the member of staff to aid in any investigation.

**11.5** The School advises staff to keep their account privacy as high as possible. Any contact from a pupil, or attempted contact, must be immediately reported to the school safeguarding lead. Staff should not respond to any contact / request for contact from any pupil other than to delete / block.

**11.6** As a professional, you must remember that in addition to protecting yourself, you should not participate in anything via social media that would bring your employer into disrepute.

**11.7** All staff are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

**11.8** Staff are encouraged to be wary about publishing specific and detailed private thoughts online. A general rule is don't post/share/tweet/re-tweet anything you would not be happy for your Principal to see.

## 12 Mobile technologies

**12.1** Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and Internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

## 13 Personal Mobile devices (including phones)

**13.1** The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil using their personal device.

**13.2** The school advises staff not to contact parents or carers using their personal device.

**13.3** The school is not responsible for the loss, damage or theft of any personal mobile device.

**13.4** The sending of inappropriate text messages between any members of the school community is not allowed.

**13.5** Whilst on the premises or while conducting official school business, permission must be sought before any image or sound recordings are made on personal devices by any member of the school community.

**13.6** Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

**13.7** While in school, personal mobile phones shall be set on discreet mode.

**13.8** Mobile phones shall only be used in work in accordance with instructions issued by the school's mobile phone guidelines.

## 14 School provided devices (including phones)

**14.1** Where the school provides mobile technologies such as phones or laptops for offsite visits and trips, only these devices should be used to conduct school business.

**14.2** Fixed telephony equipment must not be moved, unplugged or switched off except with the express permission of ICT Support.

**14.3** Settings on telephones must not be altered as this could cause a failure to ring. Proper use of divert or follow me facilities is permitted.

**14.4** Personal incoming calls (by landline or mobile) or faxes with the exception of emergencies whilst at work, should be discouraged and where unavoidable must be kept to a minimum.

## 15 Taking of Images and Film

**15.1** Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

**15.2** With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

**15.3** Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Principal, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

## 16 Publishing pupils' images and work

**16.1** On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- On the school website;
- On the school's Twitter/Instagram pages;
- In the school prospectus and other printed publications that the school may produce for promotional purposes;
- Recorded/transmitted on a video or webcam;

- In display material that may be used in the school's communal areas;
- In display material that may be used in external areas, i.e. exhibition promoting the school;
- General media appearances, e.g. local / national media / press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

**16.2** This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

**16.3** Parents / carers may withdraw permission, in writing, at any time. Consent has to be given by both parents / carers in order for it to be deemed valid.

**16.4** Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published.

**16.5** Before posting student work or images external to the school, e.g. on the Internet or distributing to the Press, a check needs to be made to ensure that permission (from the parents and the pupil) has been given for work to be displayed. This is the responsibility of the member of staff submitting the information.

## 17 Storage of Images

**17.1** Images / films of children are stored only on the school's network. Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Principal. Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network / Learning Platform. Images must be deleted when they are no longer required.

## 18 Webcams and CCTV

**18.1** The school uses CCTV for security and safety. Notification of CCTV use is displayed at the front of the school.

We do not use publicly accessible webcams in school. Webcams in school are only ever used for specific learning purposes. Consent is sought from parents / carers and staff on joining the school, in the same way as for all images.

## 19 Complaints

**19.1** Complaints relating to e-safety should be made to the Principal. All incidents should be logged.

## 20 Inappropriate material

**20.1** All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the ICT Network Manager.

**20.2** Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Network Manager.

# Acceptable Use Agreement

This is the Acceptable Use Agreement for our school. The purpose of this policy is to promote positive and responsible network and Internet behaviour. Please read carefully; by acknowledging on CPOMs that you have read this policy, you will be indicating that you agree to the terms set out below.

**Staff:**

- I will only use school IT systems, external logins and email for school related purposes. Other use will be with the permission of SLT.
- I will not divulge any school related passwords and I will comply with school IT security procedures.
- I will make sure email with staff, parents, pupils and members of the public are responsible and in line with school policies.
- I will not give my home address, phone number, mobile number, personal social networking details or personal email address to pupils.
- I accept that pupils may find these details out, and that any contact should be logged and either not reciprocated, or replied to in line with school policies. I should be responsible and aware of my professional responsibilities and school policies if I supply any personal details to parents.
- I will use school email systems for school related communications. I will not use personal accounts for school business.
- I will ensure that personal data is stored securely and in line with the Data Protection Act / GDPR. I will follow school policy with regard to external logins, encrypted data and not storing school material on personal IT equipment.
- I will not install software onto workstations or the network unless supervised by the Network Manager or IT support staff.
- I will not search for, view, download, upload or transmit any material which could be considered illegal, offensive, defamatory or copyright infringing using school IT equipment.
- Photographs of staff, pupils and any other members of the school community will not be used outside of the internal school IT network unless written permission has been granted by the subject of the photograph or their parent / guardian. I will ask the permission of the Principal (on site) or the proprietor of the building (off site) prior to taking any photographs.
- I am aware that all network and Internet activity is logged and monitored and that the logs are available to SLT in the event of allegations of misconduct.
- I will not write or upload any defamatory, objectionable, copyright infringing or private material, including images and videos, of pupils, parents or staff on social media or websites in any way which might bring the school into disrepute.
- I will make sure that my Internet presence does not bring the teaching profession into disrepute and that I behave online in line with school policy.
- I will champion the school's e-safety policy and be a role model for positive and responsible behaviour on the school network and the Internet.
- I will not make comments about school on personal social media, whether positive or negative.
- I will not use my personal phone or camera to take photographs of pupils even if this is for a school purpose.