"Inspiring a love of lifelong learning"

ICT and Digital Safety Policy

Policy date: Spring 2019
Review date: Spring 2021

Learning at Charville is underpinned by our Core Values

Respect

Independence

Self-belief

Honesty

Caring

Determination

CONTENTS

1. Scope

1.1. This policy applies to school based employees who are directly employed by the school. It applies to all users of the school's network, and the use of the school's computer facilities, (including telephony, hardware, software, e-mail, internet, etc.) used anywhere, for professional or personal purposes whether in working time or in the employee's own time.

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
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook (school page) and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

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 and that some have minimum age requirements, usually 13 years.

1.4 At Charville we understand the responsibility and are committed to educating our pupils on digital 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 Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities in line with GDPR. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

1.6 Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

1.7 This policy is inclusive of both fixed and mobile internet technologies provided by the school (such as PCs, laptops, mobile devices, 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, and other mobile devices).

2. Aim

The purpose of this policy is to:

2.1. Protect employees by making clear what acceptable use of the school's computer facilities is.

2.2. Protect employers by making clear what acceptable use of the school's computer facilities is.

2.3. Protect the security and integrity of the school and its computer facilities.

2.4. Educate our pupils on digital 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.

3. Policy

3.1. High standards of conduct are as relevant to the use of the school computer facilities as they are to all other aspects of work, and employees must conduct themselves in line with the school's code of conduct and disciplinary code.

3.2. Employees who are in any doubt about what is, or is not, acceptable use of the school's computer facilities must seek advice from their manager or the designated ICT person in advance of the use.

3.3. Employees must conduct themselves honestly, appropriately and in accordance with the law and this policy when using the school's computer facilities.

3.4. Breach of this policy may lead to disciplinary action and result in withdrawal of access to some or all computer facilities. Serious breaches may be regarded as gross misconduct and

may lead to dismissal. Employees are required to sign a statement agreeing to the terms and conditions of this policy.

3.5. The school will co-operate with any law enforcement activity.

3.6. Managers must ensure that employees have the skills to use the school's technology.

3.7. The school will purchase all hardware and software through approved suppliers.

4. Access

4.1. The school provides access to ICT to enable employees to undertake their duties.

4.2. The Head Teacher or another designated senior person has authority to obtain access to an employee's data and documents.

5. Monitoring

5.1. Each employee will be required to read and sign the ICT and Digital Safety Policy at start of employment and bi-annually every September.

5.2. Staff and Governors who are provided with school laptops will also need to read, sign and comply with the 'Staff / Governor Laptop Policy'.

5.3. Authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the General Data Protection Regulation Act 2018, or to prevent or detect crime.

5.4. The school's computer facilities will be monitored to ensure this policy is adhered to and that these facilities are used properly.

5.5. Any information (including personal emails, documents, etc.) within the school's network or equipment can be inspected, at any time, without notice.

6. Breaches and Incident Reporting

6.1. A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

6.2. Any policy breach is grounds for disciplinary action in accordance with the school Behaviour Policy.

6.3. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT in school must be immediately reported to the Head Teacher.

7. Roles and Responsibilities in Digital Safety

7.1. As Digital Safety is an important aspect of strategic leadership within the school, the Head and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Digital Safety co-ordinator in this school is the Head Teacher who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post.

7.2. Senior Management and Governors are updated by the Head and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

7.3. This policy, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Child Protection, Health and Safety, and Behaviour (including the anti-bullying) Policy and PSHE.

8. Digital Safety in the Curriculum

8.1. ICT and online resources are increasingly used across the curriculum. It is essential for digital safety guidance to be given to the pupils on a regular and meaningful basis.

8.2. Digital safety is embedded within our curriculum and staff continually look for new opportunities to promote digital safety.

8.3. Digital safety is a fundamental part of the school's Computing curriculum, with each lesson identifying aspects of digital safety which pupils must be made aware of during the teaching input for all Computing lessons.

8.4. The school has a framework for teaching internet skills in Computing/Social, Moral, Spiritual and Cultural lessons.

8.5. The school provides opportunities within a range of curriculum areas to teach about digital safety, including Staying Safe and Anti-Bullying week.

8.6. Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the digital safety curriculum.

8.7. Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

8.8. Pupils are aware of the impact of cyberbullying/online bullying through the curriculum and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher, pastoral team or trusted staff member.

8.9. All staff are encouraged to incorporate digital safety activities and awareness within their curriculum areas. Staff aim to embed digital safety messages across the curriculum whenever the internet and/or related technologies are used.

9. General Use of Email

9.1. The use of e-mail within most schools is an essential means of communication for all staff. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. Staff recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette.

9.2. The school gives all staff and governors their own e-mail account (@charvilleacademy.org) to use for all school business as a work based tool. This is to protect staff and governors and

minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

9.3. Only school approved, secure e-mail system(s) are to be used for school business

9.4. Personal email addresses should not be distributed under any circumstance to pupils or parents.

9.5. Passwords should include a capital letter, lower case letters and a number or symbol and must remain private to the individual. If passwords have been forgotten then individuals must contact the schools' ICT technician for a password reset.

9.6. Staff must inform the Head Teacher and Deputy Head Teacher if they receive an offensive e-mail.

9.7. Pupils are introduced to e-mail as part of the Computing Scheme of Work.

9.8. Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.

9.9. However school e-mails are accessed (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

9.10. Staff should report any suspected 'phishing' or viruses attached to emails to IT Support or the IT Co-ordinator.

10. Sending and Receiving Emails

10.1. **When sending emails staff should remember that if sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies to:**

10.1.1. Use their Charville email account (if you have assigned rights) so that member of staff is clearly identified as the originator of a message.

10.1.2. Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.

10.1.3. Remember that school e-mail is not to be used for personal advertising or any other personal purposes.

10.1.4. Use pupil's initials as opposed to pupil names in their emails for child protection purposes.

10.2. **When receiving emails staff are expected to:**

10.2.1. Check e-mails regularly, to never open attachments from an untrusted source and to consult their network manager first.

10.2.2. Not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.

10.2.3. Remember that the automatic forwarding and deletion of e-mails is not allowed.

10.3. **When sending personal, sensitive and classified information via email staff are expected to:**

10.3.1. Obtain express consent from your manager to provide the information by e-mail.

10.3.2. Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail.

10.3.3. Verify the details, including accurate e-mail address, of any intended recipient of the information.

10.3.4. Verify (by phoning) the details of a requestor before responding to e-mail requests for information where there are any concerns about the individual/s.

10.3.5. Not copy or forward the e-mail to any more recipients than is absolutely necessary.

10.3.6. Not send the information to anybody/ person whose details you have been unable to separately verify (usually by phone).

10.3.7. Send information as an encrypted document attached to an e-mail.

10.3.8. Provide the encryption key or password by a separate contact (non-email) with the recipient(s).

10.3.9. Not identify such information in the subject line of any e-mail.

10.3.10. Request confirmation of safe receipt.

11. Acceptable Use of ICT Facilities

11.1. **This section of the policy outlines areas of acceptable use that you agree to along with the rest of this policy on signing.**

11.2. The school's email / Internet / Internal online systems / Learning Platform / WiFi and any related technologies are only to be used for professional purposes or for uses deemed 'reasonable' by the Head and Deputy Head

11.3. You must ensure that all electronic communications, including social networking is compatible with your professional role.

11.4. You must ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Deputy Head. Personal or sensitive data taken off site must be encrypted

11.5. Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with the written consent of the parent, carer or staff member.

11.6. You must support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.

11.7. You agree to ensure that your online activity, both in school and outside school, will not bring your professional role of the school into disrepute.

11.8. You agree to support and promote the school's ICT and Digital safety policie and help pupils to be safe and responsible in their use of ICT and related technologies.

12. Inappropriate Use of ICT Facilities

12.1. **Employees must not use the school's computer facilities to:**

12.1.1. Send or access messages that are, or perceived to be, libellous, harassing or defamatory, or cause offence to the dignity of an individual or group.

12.1.2. Send personal emails from a personal address using a school computer/ device.

12.1.3. Access inappropriate internet sites or material. These may include pornographic, racist or any other sites not appropriate for a school. In the case of accidental access, the employee must immediately disconnect and inform their manager.

12.1.4. Store, view, print or redistribute any inappropriate material that could also be considered offensive, illegal or discriminatory.

12.1.5. Access chat rooms, social networking sites or newsgroups for personal use.

12.1.6. Advertise or send personal messages to large groups internally or externally unless through a specified facility or with the permission of an authorised person.

12.1.7. Spread harmful programmes that may damage the school's computer facilities.

12.1.8. Install any hardware or software without permission of the Head Teacher / Deputy Head and work is to be carried out by the IT technician or ICT Lead following the receipt of a ticket.

12.1.9. Download, use or distribute software including entertainment software or games without first consulting the IT technician / Head Teacher / Deputy Head.

12.1.10. Download video and audio streaming for personal purposes.

12.1.11. Use their school e-mail address for the purchase of personal goods or personal financial transactions.

Images of pupils and/ or staff will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head Teacher.

13. Live Technology and CCTV

13.1. The school uses CCTV for security and safety. The only people with access to this are the site manager, the Head Teacher and Deputy Head Teacher. Notification of CCTV use is displayed at the front of the school. Please refer to the hyperlink below for further guidance https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf.

13.2. Publicly accessible webcams are not available in school.

13.3. Webcams/videos/streaming in school are only ever used for specific learning purposes, i.e. monitoring hens' eggs and never using images of children or adults.

13.4. Staff must ensure any live technologies are pushed into the closed position at all times on school computers and not left open at any time.

.

13.5. Misuse of the live technologies by any member of the school community will result in sanctions.

13.6. Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.

14. School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

14.1. As a user of the school ICT equipment, you are responsible for your activity.

14.2. ICT equipment (e.g. iPads) must be signed out, returned, charged and signed back in to the ICT cupboard. Charger cables are not to be taken unless permission from the ICT co-ordinator, Head teacher or assistant head is sought.

14.3. Mobile devices must be stored within a lockable cupboard in the classroom or on the corridor.

14.4. Staff are made aware that ICT equipment is their responsibility if signed out to use in class.

14.5. Staff must ensure that their classroom is locked if leaving ICT equipment unattended.

14.6. Charville logs ICT equipment issued to staff and records serial numbers as part of the school's inventory.

14.7. Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the guest wireless ICT facilities if available.

14.8. Ensure that all ICT equipment that you use is kept physically secure.

14.9. Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.

14.10. It is imperative that you save your data on a frequent basis to the school network. You are responsible for the backup and restoration of any of your data that is not held on the school's network.

14.11. Personal or sensitive data should not be stored on the local drives of school or personal desktop PC, laptop, USB memory stick, or other portable device. If it is necessary to do so the local drive or USB must be encrypted.

14.12. Privately owned ICT equipment should not be used on a school network.

14.13. On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled.

14.14. It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.

14.15. All ICT equipment allocated to staff must be authorised by the appropriate Line Manager.

14.16. Authorising Managers are responsible for:

14.16.1. Maintaining control of the allocation and transfer within their team.

14.16.2. Recovering and returning equipment when no longer needed.

14.16.3. All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).

15. Portable & Mobile ICT Equipment

15.1. This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

15.2. All activities carried out on school systems and hardware will be monitored in accordance with the general policy.

15.3. Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted.

15.4. Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.

15.5. Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis.

15.6. Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

15.7. The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support.

15.8. In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

15.9. Portable equipment must be transported in its protective case if supplied.

16. Mobile Technologies

16.1. 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 or parent/carer using their personal device.

16.2. Under no circumstances should personal mobile phone numbers be given out to pupils or parents.

16.3. Pupils in Year 6 are allowed to bring personal mobile phones to school but must not use them for personal purposes within school. These are collected at the start of the school day and reissued at dismissal.

16.4. At all times the device must be switched onto silent.

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

16.6. The sending of inappropriate text messages or instant messaging services (including but not limited to WhatsApp) between any members of the school community is not allowed.

16.7. Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.

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

16.9. Staff are not permitted to use their phones around school during the school teaching hours. However, senior staff, the Head Teacher's PA, Pastoral team, Site Manager and Assistant Site Manager are required to carry their phones around site in the event of an emergency.

17. School Provided Mobile Devices

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

17.2. Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.

17.3. Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used.

17.4. Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

18. Confidentiality and Security of Data

18.1. The school is legally responsible for all information stored or transmitted by its computer systems and for any improper disclosure. Disclosure of data, even unintentionally, can breach the Data Protection Act and GDPR. Security measures are in place to ensure the confidentiality of data held by the school and employees are accountable for breaches of security or confidentiality.

18.2. Employees must not attempt to disable or evade any security facility.

18.3. User IDs and passwords must be kept secure and confidential, and passwords changed if an unauthorised person may be aware of them.

18.4. Employees must carefully address e-mails to avoid sending sensitive information to the wrong recipient.

18.5. Employees must ensure that data they are storing, updating or transmitting is accurate, and must not amend or alter e-mails they receive.

18.6. To ensure security it may be necessary to prevent machines with sensitive data from connecting to the internet, or restrict usage of file transfers.

18.7. Employees must use the appropriate system/method e.g., password-protected lock screen, if leaving their computer for short periods and switch computers off at the end of the working day .

18.8. Under GDPR passwords must contain a minimum of seven characters and not be part of the users' name.

18.9. Passwords must contain a mixture of 3 of the following: upper and lowercase letters, numbers and symbols.

18.10. If employees are aware of a breach of security with their password or account inform the Head Teacher or Deputy Head Teacher immediately as well as IT Support.

19. Copyright, Legal and Contractual Issues

19.1. Downloading and copying data and software or sending the work of others to third parties without permission can infringe copyright. The school retains the copyright to any original ICT based material produced by an employee in the course of their duties.

19.2. Copyright should be checked and appropriate permissions sought. In the case of subscription services the appropriate licenses must be obtained.

19.3. Software can only be downloaded with permission from the Head Teacher or the designated authorised ICT person. Downloaded software becomes the school's property and must be used only under the terms of its license. Employees must arrange to license and register such software, where required. Software downloaded without permission must be deleted.

19.4. Employees must not transfer any software licensed to the school or data owned or licensed by the school without authorisation from the Head Teacher or the designated ICT person.

19.5. The use of computer facilities can lead to contractual obligations in the same way as verbal or written transactions. Employees must not exceed their delegated authority to enter into contracts or authorise expenditure.

19.6. Records of computer transactions must take place through archiving or backup. Where appropriate, confirmation of receipt of important e-mails must be gained which may be disclosed in litigation.

19.7. Transactions through computer facilities must be treated in the same way as transactions on the schools headed paper.

20. Network Efficiency and Computer Viruses

20.1. Employees must regularly delete or archive files no longer required or needed for immediate access in line with GDPR.

20.2. All files will be scanned for viruses.

20.3. Wherever possible intensive operations such as large file transfers, video downloads, mass e-mailing should be scheduled during off-peak hours.

20.4. Video and audio streaming and downloading must be for work purposes only.

20.5. All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick, must be checked for any viruses using school provided anti-virus software before being used.

20.6. Never interfere with any anti-virus software installed on school ICT equipment that you use.

20.7. If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.

20.8. If you suspect there may be a virus on any school IT equipment, stop using the equipment, unplug all power and network cables immediately and contact your IT support provider. The IT support provider will advise you what actions to take and be responsible for advising others that need to know.

21. Software

21.1. The school must ensure all software is legally licensed and is responsible for managing and maintaining the register of software and for holding licenses and the original media.

21.2. No software can be loaded onto or used on any computer owned or leased unless approved by and licensed to the school.

21.3. All software must be procured by the school and installed by the designated authorised ICT person.

21.4. Software must not be copied or distributed by any means without prior approval from the Head Teacher or the designated authorised IT person.

22. Telephone Services

22.1. Staff are responsible for the security of their school mobile phone.

22.2. A PIN code must always be set on your school mobile phone and not left unattended or on display (especially in vehicles). This is required in order to access your staff email account on your phone.

22.3. Staff must read and understand the user instructions and safety points relating to the use of their school mobile phone prior to using it.

22.4. All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default.

23. Social Media including Class Dojo

23.1. Charville uses social media to communicate with parents and carers.

23.2. Staff are responsible for all postings on these technologies and monitor responses from others.

23.3. Senior staff and approved teaching staff are permitted to use the school Wi-Fi to access, update and post on social media for school related posts.

23.4. Staff are not permitted to access their personal social media accounts using school equipment at any time during the school day.

23.5. Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

23.6. Due to restrictions from filtering on school internet and Wi-Fi, social media websites are blocked on school computers and on all devices connected to school Wi-Fi.

23.7. Please see the Social Media Policy for more details about this.

24. Authority to Express Views

24.1. Employees using school computer facilities must communicate the school's, and not their personal, views.

24.2. Employees must not participate in newsgroups/chat rooms/social networking sites, unless in a professional capacity relevant to their duties and with prior agreement from their manager or the designated authorised person.

24.3. Employees must not use the school or its name to endorse any non-school commercial product or service.

25. Parental Involvement

25.1. Charville believe that it is essential for parents/carers to be fully involved with promoting digital safety both in and outside of school and to be aware of their responsibilities. Staff should regularly consult and discuss digital safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies together with the associated risks.

25.2. The school disseminates information to parents relating to digital safety where appropriate in the form of;

- Information and celebration evenings
- Practical training sessions e.g. How to adjust the Facebook privacy settings
- Posters
- School website

- Newsletter items
- Letters
- Text Messages
- Social Media, e.g. Facebook page
- Class Dojo

26. Current Legislation

26.1. **Acts Relating to Monitoring of Staff email**

Data Protection Act 2018

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

https://www.gov.uk/government/publications/data-protection-act-2018-overview

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 200

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

26.2. **Acts Relating to e-safety**

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.
For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:
Access to computer files or software without permission (for example using another person's password to access files)
Unauthorised access, as above, in order to commit a further criminal act (such as fraud)
Impair the operation of a computer or program
UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

26.3. Acts Relating to the Protection of Personal Data

Data Protection Act 2018
https://www.gov.uk/government/publications/data-protection-act-2018-overview

The Freedom of Information Act 200
http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

The General Data Protection Regulation (EU) 2016/679 ("GDPR")
https://gdpr-info.eu/

27. Declaration

I have read and understood the Charville ' ICT and Digital Safety Policy' and by signing this I understand the expectations of using the device. Name: …….. Role: …….. Signature: ……..

Charville Academy is not responsible for the content of external sites.

Appendix 1

Charville Academy Laptop Policy

By reading and signing this document you MUST have first read and signed the ICT & Digital Safety Policy.

This document serves to outline Charville Academy's policy on the use and storage of your staff laptop.
This is intended to minimise Charville Academy's exposure to information security risks as well as increase the user's personal safety and safeguard the school's hardware investment.

Monitoring

- **SLT or the ICT technician can ask for your laptop at any time for random inspection. It is your responsibility to provide them with the laptop when requested**
- **A proportion of laptops will be recalled monthly. This will be a random selection of laptops. No notice will be given and laptops are expected to be in school on Tuesdays for ICT technician to monitor.**

Physical Security

Employees will be provided with a laptop when it is essential to their productivity and function. When issued with a school laptop, staff are expected, to abide to, and champion, the school's physical laptop security policy.

- **Always lock the laptop out of sight if not in use. If you cannot lock the laptop out of sight then place out of sight in a safe place.**
- **Never leave a laptop logged on to networks, email and websites. Always shut down or activate a password-protected screensaver. This can be done by holding the windows key + L on the keyboard.**

General Responsibilities

- **Don't leave laptops unattended.**
- **Always lock the laptop when not in use.**
- **Don't allow anyone else to use your laptop — it is school equipment and provides access to our networks, with the exception of assigned staff who has remote access.**
- **If left at work overnight, lock out of sight.**

At Home

- **Always store inside your home, never leave in the car and keep where it cannot be easily seen from outside. Ideally, keep locked in a cupboard or strong drawer.**
- **Do not allow any use that is not authorised by the school.**
- **Do not allow others to use the laptop. It is your responsibility.**
- **Only use in an office-like environment with table and chair. Do not be tempted to use near water.**
- **Only connect to approved or known wireless networks. Ideally use your encrypted domestic connection if available.**

In the Car

- **Your laptop is not left in the car at all.**
- **While the vehicle is in motion, your laptop should be stored in its carry bag. Ideally secure in the boot; a heavy item such as a laptop can become a hazard to vehicle occupants in an accident.**

Public Transport and Public Places.

- **Laptops are particularly vulnerable to theft and loss while using public transport. Be vigilant.**
- **Do not use your laptop while travelling unless necessary. Even then, consider the location you choose with care. Ensure you are not easily overlooked and never open documents or communications that are of a personally sensitive nature while in a public place.**
- **Never leave unattended and never allow anyone else to use your laptop.**
- **Be aware of your surroundings. Ensure you are not exposing yourself or the laptop to opportunistic theft.**
- **Only connect to approved or known wireless networks.**

Protection Responsibilities

- **The school network can only be accessed when on the school premises, unless remote access is enabled for assigned staff.**
- **Remember that access to your laptop can also mean access to the school's network when on the school's premise.**
- **Your laptop is the property of the school; do not lend it to anyone or otherwise permit use by anyone else.**
- **If you leave your laptop switched on and unattended you must activate the password protected screensaver. Ideally, never leave switched on or logged in. Log out or shut down.**

Malware, Spyware and Anti-Virus

Malware is harmful software such as viruses and spyware. Malware on your laptop could be spread to the wider school network or risk the security of the data on your laptop. It is important that no malware should be allowed on your computer.

- **The School provides all laptop teaching staff with pre-installed antivirus software. Make sure you know how to access and use this software. Ask school's ICT technician for advice if needed.**
- **If you do not have regular access to WiFi then you will not receive regular antivirus updates. Make sure you log on to the school network at least once a week to allow for these important updates to take place. If this is not possible, talk to the ICT technician about ways to keep your antivirus application definitions current.**
- **Always scan files for viruses. Your email is automatically scanned for you as are files from the school network, but if you are given a file on a disk, USB key or by any other means then you must first scan the disk and/or file for viruses.**
- **Do not open any email attachments unless they were expected and from a trusted source. Email attachments are the number-one malware risk.**
- **If you suspect a virus attack, contact the ICT technician immediately. Do not access the school network or back up files until your laptop has been inspected.**

Recovery and Backing Up of Data

If the worst should happen and your laptop is stolen, lost, damaged or simply fails then it is always possible to recover your data, but only up to your last backup. It is your responsibility to ensure that you make adequate backup provision.

- **It is advised that you restart your laptop and login at school to sync to the server and ensure back up onsite.**
- **Store backup data separately to your laptop.**
- **Contact the ICT technician if you need advice or require specialist or additional backup.**
- **Report the theft or loss of laptop to SLT or school technician immediately.**

Software

Your laptop is supplied with software. These are the only applications licensed for use. Do not try to install additional software without the express consent of the ICT technician, Head, Deputy Head or ICT Lead.

- **Be aware of websites and emails guiding you to download applications. You are not authorised to do so and downloaded applications may breach school policy and expose a serious security risk.**
- **If you need an additional application or update contact the ICT technician to discuss.**

I have read and understood the Charville Laptop Policy and by signing this I understand the expectations of using the device.

Name: ……..

Role: ……..

Signature: ……..