"Inspiring a love of lifelong learning"

IT and Digital Usage Policy

Policy date: May 2025
Review date: May 2027

Learning at Charville is underpinned by our Core Values

Respect
Independence
Self-belief
Honesty
Caring
Determination

Contents

1. Scope

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

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 IT 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
- Email, Instant Messaging and chat rooms
- Social Media, including Facebook (school page) and Twitter
- Mobile/ Smart phones/ Smartwatches 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.

Whilst exciting and beneficial both in and out of the context of education, much IT, 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.

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.

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.

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.

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:

- Protect employees by making clear what is acceptable use of the school's computer facilities.
- Protect the employer by making clear what is acceptable use of the school's computer facilities.
- Protect the security and integrity of the school and its computer facilities.
- 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. Expectations of Stakeholders

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.

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 IT person in advance of the use.

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

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.

The school will cooperate with any law enforcement activity.

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

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

4. Access

Charville Academy provides access to IT to enable the employer/ employees to undertake their duties.

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

5. Monitoring

Each employee will be required to read and sign the IT and Digital Safety Policy annually.

Each employee will be required to read and sign the Social Media Policy at the start of employment and every two years thereafter.

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

Authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, 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 IT; 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.

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

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

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

Any policy breach is grounds for disciplinary action in accordance with the school Behaviour for Learning Policy and the staff and volunteers code of conduct.

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

7. Roles and Responsibilities in Digital Safety

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 coordinator in this school is the Headteacher 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.

Senior Management and Governors are updated by the Headteacher 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 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 for Learning, Anti-Bullying and PSHCE Policies.

8. Digital Safety in the Curriculum

IT 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.

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

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.

The school has a framework for teaching internet skills in Computing and PSHCE lessons.

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

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.

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.

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.

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

The use of email within most schools is an essential means of communication for all staff. 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. Staff recognise that pupils need to understand how to style an email in relation to their age and good network etiquette.

The school gives all staff and governors their own email 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 emails and avoids the risk of personal profile information being revealed.

Only school approved, secure email system(s) are to be used for school business.

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

Passwords should be strong and must remain private to the individual. If passwords have been forgotten then individuals must contact identified staff for a password reset.

Staff must inform the Headteacher and Deputy Headteacher if they receive an offensive email.

Pupils are introduced to email as part of the Computing Curriculum.

Pupils must immediately tell a teacher/ trusted adult if they receive an offensive email.

However, and wherever, school emails are accessed (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply.

Staff should report any suspected 'phishing' or viruses attached to emails to TIO, the finance team or the Computing coordinator.

Staff are responsible for reading the daily briefing email and checking their emails at least once per working day. Information which may be important for the welfare of staff or students may be cascaded via email.

10. Sending and Receiving Emails

Staff should check emails regularly, at least once per working day and read the daily briefing email.

When sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies staff should remember to:

Comply with the requirements of the General Data Protection Regulations (GDPR).

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

Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate.

Remember that school email is not to be used for personal advertising or any other personal purposes.

When receiving emails staff are expected to:

- Never open attachments from an untrusted source without consulting the network manager (TurnItOn) first.

- Remember that the automatic forwarding and deletion of emails is not allowed without prior permission being obtained from the Headteacher.

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

- Exercise caution when sending the email and always follow these checks before releasing the email.

- Verify the details, including accurate email address, of any intended recipient of the information.

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

- Not copy or forward the email to any more recipients than is absolutely necessary.

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

- Not identify such information in the subject line of any email.

- Request confirmation of safe receipt.

- If in doubt consult the Data Protection Officer (School Business Manager).

11. Acceptable Use of IT Facilities

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

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 or Governing Body.

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

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 Governing Body. Personal or sensitive data taken off site must be encrypted.

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.

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.

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

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

12. Inappropriate Use of IT Facilities

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

- 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.
- Send personal emails from a personal email address.
- 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.
- Store, view, print or redistribute any inappropriate material that could also be considered offensive, illegal or discriminatory.
- Access chat rooms, social networking sites or newsgroups for personal use.
- Advertise or send personal messages to large groups internally or externally unless through a specified facility or with the permission of an authorised person.
- Spread harmful programmes that may damage the school's computer facilities.
- Install any hardware or software without the permission of the Headteacher, Deputy Head or Computing Lead; work is to be carried out by the TIO technician only.
- Download, use or distribute software including entertainment, software or games without first consulting the TIO technician / Headteacher / Deputy Head.
- Download video and audio streaming for personal purposes.
- Use their school email 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 Headteacher.

13. Live Technology and CCTV

The school uses CCTV for security and safety. The only people with access to this are the site manager, the Headteacher and Deputy Headteachers. 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.

Publicly accessible webcams are not available in school.

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 without permission.

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 where possible. This applies to external devices as they should be unplugged or simply faced away from the working area when not in use. Exceptions can be made by requesting permission from the Headteacher in some situations.

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

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

14. School IT Equipment including Portal and Mobile IT equipment and Removable Media

As a user of the school IT equipment, you are responsible for equipment used for your activities.

IT equipment (e.g. iPads) must be signed out, returned charged and signed back into the IT cupboard. Charger cables are not to be taken unless permission from the IT coordinator or a senior leader is sought.

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

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

Staff must ensure that their classroom door is shut if leaving IT equipment unattended.

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

Visitor are not allowed to plug their IT hardware into the school network points (unless special provision has been made). They should be directed to the guest wireless IT facilities.

All IT equipment that is used must be kept physically secure.

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.

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.

Personal or sensitive data should not be stored on the local drives of a 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.

Privately owned IT equipment should not be used on the school network but may use the wifi.

On termination of employment, resignation or transfer, return all IT equipment to the resources assistant. You must also provide details of all your system logons so that they can be disabled.

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.

All IT equipment allocated to staff must be authorised by the resource's assistant.

Authorising Managers are responsible for:

- Maintaining control of the allocation and transfer within the school.
- Recovering and returning equipment when no longer needed.

15. Portal and Mobile IT Equipment

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.

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

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

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.

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

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

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

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

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

16. Mobile Technologies

The school allows staff to bring in personal mobile phones for their own use.

Staff must not use mobile phones in view of the children for personal use.

Staff are only permitted to use their phones around school during the school teaching hours in situations where they are using it to contact other staff members for work related issues, for example, welfare, pastoral etc.

Staff members may contact a pupil or parent/carer using their personal device where appropriate and related to work. Staff should withhold their number or use a school phone to call parents where appropriate.

Mobile phone numbers should not be given out to pupils or parents unless prior permission from the Headteacher has been obtained.

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.

At all times personal devices must be switched onto silent except where this has been authorised by the Headteacher.

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

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.

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

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

Staff are required to carry their phones around the site in the event of an emergency.

Staff must obtain permission from the Headteacher in order to bring in personal devices, other than mobile phones in order to use them for work purposes.

With permission, staff using personal laptop devices are allowed access to the Wifi and printing networks as long as they are using them for work related purposes.

Staff must be vigilant when printing from personal devices as this will not be secure as it will go straight to print (not PIN protected). Where possible, staff should store files on their work Gmail or Google drive and print from a secure work computer using their personal printing code.

Staff must obtain permission from the Headteacher to access the shared drives when using personal laptop devices and where possible should instead share their work and files to themselves via their secure Gmail or Google drive.

Any materials produced on a personal device remain the property of the school and must be transferred to the school network on request or, in any case, before leaving the employ of the school.

No personal information about staff or students may be stored on personal devices.

17. School Provided Mobile Devices

The sending of inappropriate messages between any members of the school community is not allowed on school or personal devices.

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

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

18. Confidentiality and Security of Data

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.

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

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

Employees must carefully address emails to avoid sending sensitive information to the wrong recipient.

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

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

Employees must use the appropriate system/method e.g., password-protected lock screen, if leaving their computer for short periods and should switch computers off at the end of the working day. Exemptions can be made by the Headteacher in circumstances where they are required to be on.

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

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

Staff system user passwords must be reset yearly at the start of each academic year.

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

19. Copyright, Legal and contractual Issues

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 IT based material produced by an employee in the course of their duties.

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

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

Employees must not transfer any software licenced to the school or data owned or licenced by the school without authorisation from the Headteacher or the designated IT person.

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.

Records of computer transactions must take place through archiving or backup. Where appropriate, confirmation of receipt of important emails must be gained which may be disclosed in litigation.
Transactions through computer facilities must be treated in the same way as transactions on the schools headed paper.

20. Network Efficiency and Computer Viruses

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

All files will be scanned for viruses.

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

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

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

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

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

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 the Computing coordinator or TIO. The IT support provider will advise you what actions to take and be responsible for advising others that need to know.

All staff must undertake cyber security training on commencement of their employment and then yearly afterwards.

21. Software

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

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

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

Software must not be copied or distributed by any means without prior approval from the Headteacher or the designated authorised person.

22. Telephone Services

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

A PIN code or password 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.

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

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

23. Social Media

Charville uses social media to communicate with parents and carers.

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

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.

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

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

Due to restrictions from filtering on school internet and Wi-Fi, social media websites are blocked on most devices and user profiles connected to school Wi-Fi except where exceptions have been made. Anyone seeking access to social media must request permission from the Headteacher.

Please see the Social Media Policy for more details.

24. Authority to Express Views

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

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.

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

25. Parental Involvement

Charville believes 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.

The school disseminates information to parents relating to digital safety where appropriate in the form of:

- Information, celebration and consultation 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

Acts Relating to Monitoring of Staff email

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

The Telecommunications (Lawful Business Practice)
http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

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

Acts Relating to e-safety

Racial and Religious Hatred Act 2006
https://www.legislation.gov.uk/ukpga/2006/1

Sexual Offences Act 2003
https://www.legislation.gov.uk/ukpga/2003/42/contents

Communications Act 2003 (section 127)
https://www.legislation.gov.uk/ukpga/2003/21/section/127

The Computer Misuse Act 1990 (sections 1 – 3)

https://www.legislation.gov.uk/ukpga/1990/18

Malicious Communications Act 1988 (section 1)
https://www.legislation.gov.uk/ukpga/1988/27/section/1

Copyright, Design and Patents Act 1988
https://www.legislation.gov.uk/ukpga/1988/48/contents

Public Order Act 1986 (sections 17 – 29)
https://www.legislation.gov.uk/ukpga/1986/64

Protection of Children Act 1978 (Section 1)
https://www.legislation.gov.uk/ukpga/1978/37/section/1

Obscene Publications Act 1959 and 1964
https://www.legislation.gov.uk/ukpga/1964/74

Protection from Harassment Act 1997
https://www.legislation.gov.uk/ukpga/1997/40/contents

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
https://www.legislation.gov.uk/ukpga/2000/36/contents

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

27. Equal Opportunities

School staff and the Governing Board are responsible for ensuring this IT and Digital Usage policy is applied fairly and does not discriminate on any grounds. This policy should be read in conjunction with the Equalities Policy.

28. Related Policies

- Behaviour for Learning Policy
- CCTV Policy
- Data Protection Policy
- Electronic Device Policy
- Social Media Policy
- Equalities policy

Policy Approval

Written by: Joshua Maguire, Computing Lead

Approved by: Curriculum and Achievement

Date approved: May 2025

Review Date: May 2027

Appendix 1:

Charville Academy Laptop Policy

By reading and signing this document you MUST have first read and signed the IT & 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 IT technician can ask for your laptop at any time for random inspection. It is your responsibility to provide them with the laptop when requested
- 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 Tuesday for the IT 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, teaching staff accept to abide by, 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 it 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.
- 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 it locked in a cupboard or strong drawer.
- Do not allow any user 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 a table and chair. Do not use near water.
- Only connect to approved or known wireless networks. Ideally use your encrypted domestic connection if available.

In the Car

- Your laptop should not be 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 and externally to those with the Headteachers permission.
- Remember that access to your laptop can also mean access to the school's network when on the school's premises.
- 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 it switched on or logged in instead, log out or shut down.

Malware, Spyware and Antivirus

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 laptops for teaching staff with pre-installed antivirus software. Make sure you know how to access and use this software. Ask the school's Computing coordinator or TIO 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 IT 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 IT 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 backup onsite.
- Store backup data separately to your laptop.
- Contact the IT 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 IT technician or Headteacher.

- 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 IT 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: .....