****

**Acceptable Use of IT, the Internet and Electronic Communication including**

**Social Media**

|  |  |
| --- | --- |
| **Policy area:** | Human Resources |
| **Approved by:** | Board of Trustees |
| **Approval date:** | Out of Committee |
| **Implementation date:** | 11 Oct 2023 |
| **Version:** | V1 |
| **Review cycle:** | Annual |
| **Date of next review:** | Oct 2024 |
| **Publication:** | Public |

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSION CONTROL** | | | |
| **Version** | **Date** | **Author/Reviewer** | **Substantive changes since the previous version** |
| DRAFT V0.1 | June 23 | GB | Updated policy for ONE Academy Trust. Merges the previous WAT & Believe policies. |
| DRAFT V0.2 | June 23 | GB | Reformatted. |
| DRAFT V0.3 | July 23 | GB | ‘Reference to ‘wearable technology’ inserted (In addition to reference to smart watches). |
| V1 | Sept 23 | Checked by DD/JC/GB | Trustees' comments incorporated. No feedback from staff consultation |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Contents**

1. Introduction
2. Purpose and scope
3. Responsibilities
4. Disciplinary and related action

**SECTION 1 - Use of ONE Academy Trust/school IT resources**

1. Parents and visitors
2. Safe working practice
3. Loan of IT equipment
4. Health and safety guidance on using IT equipment including laptops
5. Use of trust/school IT equipment
6. Digital cameras
7. Software
8. Network access, passwords and data security
9. Encryption
10. File storage
11. Monitoring of email

**SECTION 2 - Electronic communications (including social media)**

1. Use of internet, email and other electronic communication

* Personal use of internet and email
* Email communications
* Internet access
* Accidental access to inappropriate material
* Copyright

1. Social media
2. Access to social media at work for personal use
3. School social media accounts
4. Responding to online safety incidents and concerns
5. Working from home and remote access
6. Virtual meetings
7. Remote Learning
8. Safeguarding
9. Early Career Teachers
10. Monitoring and review

**Appendices**

Appendix 1 - Employee guidance on the use of social media (summary)

Appendix 2 - Additional guidance for headteachers on the use of social media

Appendix 3 - Acceptable Use Agreement - volunteers & visitors

(*to be personalised and adapted by each school to suit their requirements)*

Appendix 4 - Acceptable Use Policy & Agreement (model) - parents/carers & pupils

(*to be personalised and adapted by each school to suit their requirements e.g. inclusion in home/school agreements and/or leaflets etc.)*

Appendix 5 - Device Loan Agreement for Pupils (model)

(*to be personalised and adapted by each school to suit their requirements e.g. inclusion in home/school agreements and/or leaflets etc.)*

1. **Introduction**
   1. ONE Academy Trust information technology (IT) resources are essential to the effective delivery of educational provision. Computers and other networked facilities, including internet access, are available to staff, pupils and some volunteers and visitors within schools. It is therefore vital that all users are aware of the trust’s policies and procedures relating to the use of IT resources. For example, a poorly administered network or weak password controls could expose the trust/school’s information to an unauthorised user, introduce a virus or compromise data security resulting in a data breach.
   2. ONE Academy Trust and the schools within the trust are making increasing use of electronic communication media (including emails, social media such as Twitter, video conferencing and online learning platforms) to communicate with parents, pupils and the wider school community and, more recently, to provide blended learning to support homeschooling during enforced self-isolation or lockdown periods.
   3. Electronic communication and social media platforms (e.g. Facebook, Instagram and gaming sites) are also used by many adults and some pupils as a means of personal communication.
   4. Pupils, parents and the public should have confidence in the trust/school's decisions and services. It is therefore important that all adults and pupils connected to ONE Academy Trust and the schools in the trust understand their responsibilities concerning appropriate communication, safeguarding and data protection. All adults connected to the trust/school in a professional or voluntary capacity must be conscious at all times of the need to keep their personal and professional lives separate.
   5. We will ensure that all members of our community are safe and responsible users of technology. We will support our staff to:

* Become empowered and responsible digital creators, users and storers of data
* Use resources and technology safely, carefully and responsibly, respecting system/password security
* Be safe and considerate online and create a community that is respectful and caring, on and offline
* Respect their position of standing in the community, the integrity of the school/Trust and their responsibilities as a trusted adult and/or colleague
  1. This policy operates in conjunction with all relevant ONE Academy Trust and school policies including:
* E-Safety Policy
* Staff Code of Conduct
* Disciplinary Policy
* Bullying and Harassment Policy
* Data Protection Policy
* Freedom of Information Policy
* Equality and Diversity Policy
* Child Protection and Safeguarding Policy
* Child on Child Abuse Policy
* Remote Learning Policy
* Behaviour Policy
* Anti-bullying Policy
* Home/school Agreements
* Photographs & Children’s Images Policy
* Working with VDU Guidance
  1. This policy complies with the following legislation and guidance. It reflects legislation at the time when it was last reviewed. Any changes in legislation will take precedence over anything printed in the policy.
* [Data Protection Act 2018](http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted)
* [The UK General Data Protection Regulation](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679)
* [Computer Misuse Act 1990](https://www.legislation.gov.uk/ukpga/1990/18/contents)
* [Human Rights Act 1998](https://www.legislation.gov.uk/ukpga/1998/42/contents)
* [The Telecommunications (Lawful Business Practice) Regulations 2000](https://www.legislation.gov.uk/uksi/2000/2699/regulation/3/made)
* [Education Act 2011](http://www.legislation.gov.uk/ukpga/2011/21/section/2/enacted)
* [Freedom of Information Act 2000](https://www.legislation.gov.uk/ukpga/2000/36/contents)
* [The Education and Inspections Act 2006](https://www.legislation.gov.uk/ukpga/2006/40/part/7/chapter/1)
* [Keeping Children Safe in Education](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1161273/Keeping_children_safe_in_education_2023_-_statutory_guidance_for_schools_and_colleges.pdf) (2023)
* [Searching, screening and confiscation: advice for schools](https://www.gov.uk/government/publications/searching-screening-and-confiscation)

1. **Purpose and Scope**
   1. This policy applies to:

* **All** ONE Academy Trust staff (permanent and temporary), all governance roles, teacher trainees and other trainees, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school or academy. ***Please note: these individuals are collectively referred to as ‘staff’ in this policy.*** 
  1. This policy sets out:
* the criteria for the acceptable use of ONE Academy Trust and/or school IT and communications system (e.g. PCs, laptops, tablets, mobile phones, wearable technology such as smart watches etc.).
* the criteria for the acceptable use of social media and online communications both professionally and personally whilst working in or with the trust and/or school.
  1. This policy is intended to ensure that:
* the academy's systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
* staff, volunteers, contractors, parents and pupils understand that their online conduct is their responsibility and must meet data protection and safeguarding requirements. Any personal or potentially personal information sent via e-mail and the internet is covered by the Data Protection Act 2018 and the provisions of the General Data Protection Regulations
* the confidentiality of pupils and other staff and the reputation of the trust and our schools are safeguarded.
  1. This policy is shared as part of the induction process for staff, regular volunteers and governors.

1. **Responsibilities**
   1. School managers have a duty of care to all staff and to ensure that they have a reasonable work-life balance and that they are able to work in a healthy and safe environment. Headteachers should therefore try to ensure that electronic working does not place greater burdens on staff in terms of either workload or response times. Headteachers should also endeavour to support any staff who are subject to abuse through any of the electronic media by effective and immediate sanctions, in the same way that it is expected that verbal and physical abuse is dealt with.
   2. Always think carefully about all forms of communication, but particularly electronic (which can be circulated widely and rapidly). If ‘thinking about it’ gives rise to any doubt, then the best advice is ‘don’t do it’.
   3. Headteachers and Designated Safeguarding Leads should understand filtering and monitoring systems in place within the school.
2. **Disciplinary and related action**
   1. Failure to follow the IT Acceptable Use Policy could result in appropriate disciplinary action being taken, which may include a warning, suspension, dismissal from the trust/school and, in the case of illegal activities, referral to the police.

**SECTION 1 - Use of ONE Academy Trust/school IT resources**

1. **Parents and visitors** 
   1. Visitors to school must be given permission by the headteacher or a senior member of staff to access the Guest WiFi.
   2. Authorisation will be granted if:

* Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the 'Friends' group or PTA)
* Visitors need to access the school’s wi-fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

1. **Safe working practice** 
   1. Staff should make careful, considerate use of the trust/school IT resources, report faults and work in a way that minimises the risk of introducing computer viruses into the system.
   2. Staff should always be vigilant to identify emails that carry malware or phishing attempts and should:

* Avoid opening attachments and clicking on links when content is not adequately explained
* Check email and names of unknown senders to ensure they are legitimate before opening the email.
* Look for inconsistencies or inappropriate style (e.g. grammar mistakes, capital letters, an excessive number of exclamation marks.)
* If a member of staff is unsure that an email they have received is safe, they should request a check by our IT service provider via the school office/It coordinator.
  1. Faults should be reported promptly to the school office/IT coordinator who will report to the IT service provider.
  2. Staff are responsible for maintaining the security of computers and networks by using only their own log-on details and not allowing other staff or pupils to use their personal passwords.
  3. Staff should ensure that machines are not left unattended when they are logged on.
  4. Staff should ensure that when using work equipment at home, other family members do not use the equipment for their personal use.
  5. Staff are responsible for the security of all the content (software and data) on any equipment allocated to them.
  6. Hardware and software provided by the workplace for staff use can only be used by members of staff and only for educational use or for the purpose of serving the functions of the Trust. Personal accounts or information such as personal photographs, files or financial information should not be accessed or stored on school devices and the Trust accepts no liability for loss of such data.
  7. Staff must not attempt to bypass any filtering and/or security systems put in place by the school/Trust
  8. Staff should not install any unlicensed software on equipment allocated to them. Downloading or accessing programmes or files that have not been authorised could result in the activation of malware and ransomware when devices are reconnected to school networks. Where there is a resultant data breach, staff may be individually liable for such a breach and may face disciplinary action. If activities are illegal this will be referred to the police. If in doubt, staff should ask IT support for guidance.
  9. Authorised administrators have a duty to ensure that access to secure areas of the trust/school websites (e.g. staff area, governor area) and/or access to school servers are secure. Permissions and passwords should provide different access as appropriate to their role.
  10. Each school within the trust will set its own approach with regard to the wearing of wearable technology such as smartwatches and this will be communicated clearly to all staff at induction and periodically thereafter. If you are permitted to wear a smartwatch in your setting you **must** ensure that it is on a ‘Do Not Disturb’ setting to ensure the device does not vibrate or display a notification during lesson times which is distracting for both the staff member, other staff and pupils. You must **never** use wearable technology such as smartwatches for taking photographs, making recordings on school premises, using the internet or using messaging services. Staff must also be conscious that pupils may be aware when messages/phone calls are being received and by whom due to the visible nature of such devices. Inappropriate usage could lead to disciplinary action being taken.

1. **Loan of IT equipment** 
   1. ONE Academy Trust IT equipment (e.g. laptop, tablet, mobile phone) is provided to users on a loaned basis and remains the property of the trust/school. The school/trust will ensure that users understand their responsibilities and will maintain a record of loans and returns.
   2. The IT equipment provided must not be used by any person(s) other than the authorised user(s) to whom it has been allocated and the property identification markings should not be removed for any reason.
   3. No addition or deletion of any software or hardware is permitted without the express permission of the headteacher or IT Coordinator.
   4. To ensure that security patches and virus definitions are up to date staff should connect laptops to the school network regularly.
   5. All reasonable care should be taken to prevent loss, damage, theft or unauthorised use of IT equipment as far as is practical. For example, a laptop, tablet or mobile phone should never be left in a vehicle overnight or other unsecured, vulnerable situation. Any loss or damage to school IT equipment should be immediately reported to the headteacher as this may constitute a data breach.
   6. When employment at the trust/school ends, staff must return all computer equipment and software to the headteacher or school office staff in full working condition. The user account and all personal work stored on the laptop must be securely deleted and the staff member will be required to sign a confirmation that this has been done.
   7. If software/hardware problems arise, a laptop or tablet may need to be restored to its original settings. Work files may be lost during the restore process, therefore it is the responsibility of all staff to ensure that backups of all files are regularly made to an external device such as the school’s networked server or an encrypted mobile device such as a hard drive.
   8. Where there is evidence that the laptop/tablet has not been used in accordance with the above guidelines, a charge may be made for the replacement or repair of any laptop/tablet whilst on loan.
   9. Where a laptop or tablet is loaned to parents/carers for the use of pupils e.g. during periods of remote learning, parents/carers must be informed of their responsibilities for the appropriate use and care of the equipment. When the loan period of the laptop or tablet ends, parents/carers must be required to return all computer equipment and software to the headteacher or school office in full working condition.
   10. As part of safeguarding training, including induction training, expectations and responsibilities in relation to filtering and monitoring will take place
   11. The school/Trust reserves the right to oversee and monitor the activity of users on school networks, systems and school devices. Our IT providers (AIT) may undertake checks on individual accounts as part of their IT monitoring responsibilities where concerns arise, e.g. inappropriate searches being detected, unusual data storage patterns. Access may be required for data protection purposes i.e. response to a Subject Access Request. We may need to check specific accounts if allegations of misuse have been made or misuse is suspected. In the latter situation, advice will be sought.
   12. Monitoring reports will be shared with the Trust Board as part of the governance annual schedule of business.
2. **Health and Safety guidance on using IT equipment including laptops**
   1. Employees should refer to the trust’s Working with VDU guidance for more detail.
   2. In the interests of health and safety, all users are advised to adhere to the following recommendations for the safe use of personal laptops. Any health and safety concerns associated with the use of laptops should be discussed with the headteacher. Further advice is available in the ONE Academy Trust Health & Safety policy.

* Sit in a chair that provides good back support to avoid backache and position the laptop/tablet directly in front of the user to avoid twisting;
* Take regular breaks from the screen to reduce eyestrain.
* Avoid using the laptop/tablet on a low table or on the lap as both of these positions will increase strain on the neck and lower back.

1. **Use of trust/school IT equipment**
   1. Users who borrow equipment from the trust/school must sign for it and take responsibility for its care. Loan equipment should be concealed and stored securely when not in use. Any loss or damage to equipment on loan should be immediately reported to the headteacher or IT Coordinator in the first instance, and any theft or criminal damage should also be reported to the police.
   2. To prevent data loss and ensure consistent application of school policies no personally owned equipment should be attached to the trust/school network without the permission of the headteacher of the relevant school. All mobile devices must be encrypted or password-protected wherever technology allows.
2. **Software** 
   1. Users should use software in accordance with applicable licence agreements. To copy software or any supporting documentation protected by copyright is a criminal offence. The use or possession of unlicensed copies or "pirated" versions of software is illegal and is expressly prohibited by the trust. Under no circumstances should any user possess unlicensed software on school premises or use unlicensed software on trust/school IT equipment (including portable equipment).
3. **Digital cameras and taking photographs** 
   1. Our schools encourage the use of digital cameras, iPad recordings and video equipment where appropriate to record events, activities and achievements. However, staff should be aware of the following guidelines:

* Photos should only be named with the pupil’s name if they are to be accessible in school only.
* Photos for the website or press must only include the child’s first name and parent's permission must be given prior to publishing.
* The use of personal digital cameras in school is not permitted
* All photographs/videos should be downloaded to the school network for storage
* The use of personal mobile phones or wearable technology such as smartwatches for taking photographs/videos of pupils is not permitted.

1. **Network Access, Passwords and Data Security** 
   1. Users must only access information held on the trust/school’s computer systems if properly authorised to do so and the information is needed to carry out their work. Under no circumstances should personal or other confidential information be held on the school network or IT equipment be disclosed to unauthorised persons. If you accidentally access information which you are not entitled to view, report this immediately to the headteacher or school IT Coordinator.
   2. Staff using computers in classrooms must ensure that sensitive data is not accessible to students or other individuals by logging off or locking the computer as appropriate. In other areas, computers must not be left logged on when left unattended.
   3. Staff passwords must be kept secure. System and administration level passwords should also be changed on a termly basis as a minimum.
   4. All passwords are to be treated as sensitive, confidential information. Therefore, staff must not:

* Write down passwords or store them online.
* Use school user account passwords for other types of access
* Reveal a password over the phone or in an e-mail message or other correspondence.
* Talk about a password in front of others including family members.
* Hint at the format of a password (e.g., "my family name").
* Reveal a password on questionnaires or security forms.
* Insert passwords into e-mail messages or other forms of electronic communication.
  1. If an account or password is suspected to have been compromised, the incident must be reported immediately to the headteacher or school IT Coordinator so that the account password can be changed.

1. **Encryption** 
   1. Sensitive or confidential information held on laptops or other portable devices (e.g. memory sticks) should be minimised and avoided wherever possible, and only used when issued by the trust/school and appropriately encrypted. Staff should clarify with the headteacher/data protection officer the nature of the material that may be held on these devices, for how long and with what security measures. Where the use of a memory stick to transfer or store data temporarily is unavoidable, this must be done with extreme care, following the trust’s security protocol and using an encrypted memory stick provided by the trust/school, where required.
2. **File storage** 
   1. Each member of staff has their own personal area on the school network, as well as access to shared network drives.

* Any school related work should be stored on one of these network drives.
* Personal files are not permitted on the network areas.
* Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files.
* Any files stored on removable media must be stored on an encrypted pen drive
* No school data is to be stored on a home computer, or un-encrypted storage device.
* No confidential, or school data which is subject to the Data Protection Act should be transferred off-site unless it is sent by secure email or stored on an encrypted device.
* Personal information about children which is no longer needed for a particular purpose should be deleted from the file (for example, group lists, test scores no longer needed)

1. **Monitoring of email**
   1. The trust/school’s email system automatically records details of all email sent both internally and externally. The automatic system highlights the use of certain prohibited words and any potential infringement will be referred to the headteacher/CEO as part of the routine monitoring procedures and may result in disciplinary action.

The following details are recorded in respect of every email message:

* name of the person sending the email,
* the email addresses of all recipients and copy recipients,
* the size and name of any file attachments,
* the date and time sent,
* a copy of the email,
* a copy of file attachments.
  1. The IT support provider (AIT) and an appropriate responsible person within the organisation may read and inspect individual emails and attachments for specific business/HR/legal purposes including:
* Establishing the content of transactions,
* Ensuring staff are complying both with the law and this policy
* Checking email when staff are on leave, absent or for other supervisory purposes.
* To respond to a Subject Access Request or Freedom of Information Request
  1. The purpose for accessing emails must be clearly demonstrable. See paragraph 7.11
  2. Suspected misuse of the trust/school’s computer systems by a member of staff will be considered by the headteacher or CEO as appropriate.

**SECTION 2 - Electronic communications**

***(including email, social media and video conferencing for meetings and remote learning)***

1. **Use of internet, e-mail and other electronic communications** 
   1. Internet and email use are integral to the effective delivery of educational services provided by the trust. Nothing in this policy should be read as restricting the proper use of email and the internet for trust/school activities.
   2. Every member of staff is provided with a school email address. The email system can be accessed from both the school computers and via the internet from any computer. Wherever possible all school related communication must be via the school email address.

**Personal use of internet and email**

### Limited personal use of the trust/school internet and email system is permitted subject to these principles and guidance notes.

* Email: Staff and volunteers are allowed limited use of the trust/school email for personal communication
* Internet: Personal use of the trust/school internet is permitted outside normal working hours
  1. Any personal use of email or internet must not, in any way, distract from the effective performance of their duties
  2. Staff and volunteers must not connect personal devices (e.g. a mobile phone) to the trust/school internet connection for their personal use.
  3. Staff and volunteers are not allowed to use school tablets/iPads for any personal internet activity as these are for education purposes and work-related research only.
  4. Use of e-mail and the internet (including social media), which brings the trust/school into disrepute, may result in appropriate disciplinary action.
  5. Access to personal email accounts should be in staff members' own time. Limited use of email during the working day is allowed, but is restricted to responding to urgent incoming email only and must never be used when teaching or supervising pupils. Excessive use of personal email during the working day may result in disciplinary action.
  6. Staff should not engage in social interaction using electronic means during working time (e.g. through instant messaging or on social media).
  7. While personal use of the internet and email is permitted during lunch breaks and out of working hours, staff and volunteers should be aware that the facilities are provided by the trust/school and any activity received/sent through the trust/school network, personal or otherwise, is recorded and may be monitored.
  8. Trust/school equipment should not be used to access the internet for trading or personal business purposes. Use of the internet to buy goods or services for personal use will not render the trust/school liable for default of payment or the security of any personal information disclosed. Staff and volunteers should not use the trust/school’s computer system for making personal payments.Personal goods ordered to be delivered to work addresses should be agreed in advance with the school office staff.
  9. The trust/school’s facilities must never be used for the passing of inappropriate personal information of any kind.

**Email communications**

* 1. Staff should remain aware of their professional position when communicating via email.
  2. When email is used to communicate with parents or carers as part of a professional role, a trust/school email address should always be used.
  3. The style and format of any email communication should be strictly professional. Improper statements in email can give rise to personal liability and liability for the trust/school and may constitute a serious disciplinary matter. Emails that embarrass, misrepresent or convey an unjust or unfavourable impression of the trust/school or its business affairs, staff, suppliers and their families are not permitted. Staff must not use e-mail in any way that is insulting or offensive.
  4. Staff should consider whether it is advisable to copy a colleague into any contact with a parent as a further safeguard (subject to data protection considerations).
  5. Staff are NOT permitted to communicate with pupils directly via email.
  6. Staff should be aware that email is not always the best form of communication and should consider alternatives, as appropriate.
  7. Extreme care must be taken when using the trust/school’s email facilities to transmit information. Confidential or sensitive information should not be sent via the internet or email unless the data is protected by the trust/school’s secure provision for such communications. Staff should remember that when a Subject Access Request or Freedom of Information request is submitted, relevant email communications will be included in the material to be provided.
  8. In accordance with Data Protection legislation, emails should be deleted when they are no longer required for official records in accordance with the principle of data minimisation. Each school within ONE Academy Trust follows a data retention policy which sets out the retention periods for the different categories of data.
  9. Staff must not deliberately view, copy or circulate any material that:
* could constitute bullying
* is sexually explicit or obscene
* is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
* contains material the possession of which would constitute a criminal offence
* promotes any form of criminal activity
* contains unwelcome propositions
* contains images, cartoons or jokes that will cause offence
* appears to be a chain letter
  1. There should be no expectation, other than by agreement, that staff will be available outside normal working hours because they can access emails from home. There will therefore be no expectation, other than by agreement, that staff will respond to email or other messages, sent outside the working day, before the start of the next working day. This should be made clear to parents.

**Internet access**

* 1. Many internet sites contain unacceptable content. Staff must not deliberately view, copy or circulate any material that:
* is sexually explicit or obscene
* is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
* contains material, the possession of which would constitute a criminal offence
* promotes any form of criminal activity
* contains images, cartoons or jokes that will cause offence
* that constitutes bullying
  1. Staff must make every endeavour to protect pupils from harmful or inappropriate material accessible via the internet or transportable on computer media. Internet sites used for curriculum purposes must be checked by staff before lesson delivery.

**Accidental Access to Inappropriate Material**

* 1. Many internet sites that contain unacceptable content are blocked automatically by the trust/school’s filtering systems. However, it is not possible to block all ‘unacceptable’ sites electronically in all circumstances. If staff become aware of any sites that require re-categorising they should inform the trust/school IT Coordinator as soon as possible who will then inform the IT services provider.
  2. Staff or pupils may receive an e-mail or visit an internet site that contains unacceptable material. If this occurs, a line manager or the headteacher should be informed as soon as possible. The staff member should ensure a short, written record is kept as they may be asked to provide details relating to the incident and an explanation of how it occurred. This information may be required later for management or audit purposes.

**Copyright**

* 1. Staff may violate copyright law if text is simply cut and pasted into another document. This may equally apply to photographs and music samples used as illustration or backing tracks in resource materials. Teachers should make it clear to pupils that care should be taken when including this type of material in any schoolwork. Most sites contain a copyright notice detailing how material may be used. If in any doubt about downloading and using material for official purposes, legal advice should be obtained. Unless otherwise stated on the site all downloaded material must be for curricular or research purposes and must not be passed to third parties.
  2. Downloading video, music files, games, software files and other computer programs for non-work-related purposes is not allowed. These types of files consume large quantities of storage space on the system and may violate copyright laws.
  3. No software or apps should be downloaded for use without the prior permission of the headteacher/CEO as appropriate. All purchases of software or apps must have formal prior approval at the appropriate level of financial delegation.

1. **Social Media**
   1. For the purposes of this policy, social media is defined as a type of interactive online media that allows parties to communicate instantly with each other, or to share data in a public forum. This includes online social forums such as Twitter, Facebook, Instagram, LinkedIn, internet newsgroups, and chat rooms. Social media also covers blogs and video/image-sharing websites such as YouTube and Flickr. There are many more examples of social media than can be listed here and this is a constantly changing area. These guidelines should be followed in relation to any social media used.
   2. As well as bringing many positive benefits, there are also many potential problems in utilising social media, both professionally (e.g. school Twitter account) and personally (e.g. Facebook or Instagram account). Online conduct can have an impact on the role and reputation of staff members.
   3. The following guidance is given to all staff and volunteers for their protection. The guidance should apply whether the individual is using trust/school equipment or their own equipment. The personal use of social networking sites using trust/school equipment is not permitted on school premises.
   4. At all times, staff and volunteers (including trustees and governors) should behave in accordance with the code of conduct expected of professional adults working with children. All staff are expected to behave appropriately and responsibly and should be aware that they may be accountable to the trust/school for actions outside of their work.
   5. Safe and responsible use of social media will be discussed with all members of staff as part of induction and revisited regularly. This document describes safe and professional behaviour in relation to social media.
   6. Staff who work directly with members of the public, including parents, need to be aware that the information they post on social media can make them identifiable to members of the wider trust/school community as well as people they know in a private capacity. Staff should therefore consider this when setting up a profile, particularly in relation to the use of a photograph and/or providing details of their occupation, employer and work location. Online sites such as Facebook are in the public domain, and personal profile details can be seen by anyone, even if users have their privacy settings on the highest level. Also, if a user’s profile is linked to other sites, any changes to their profile will be updated there too. Staff/volunteers who have set their privacy level to the maximum can have their privacy compromised by ‘friends’ who may not have set their security to the same standard and therefore comments, photographs or video clips sent to such contacts may be more widely available than originally anticipated. Staff must be aware that disgruntled parents or member of the community could ‘tag’ their account to issues that they believe exist in school (e.g. bullying). The school/trust will advise a personal referral to the police and social media platform administrators in the event of such an occurrence.
   7. Staff and volunteers should consider very carefully any potential conflict of interest that could arise when linking through social media to people they also know through work/their role in the trust/school. The trust considers it inappropriate to have pupils as ‘friends’ through social media, and consequently, to do so may be considered to be a disciplinary matter.
   8. All staff should be aware of the image they are presenting when communicating via social media and ensure, as far as possible, that any comments made are not open to misinterpretation. Circulation of comments on social media can be rapid and widespread and therefore staff should be encouraged to adopt the general premise of not putting anything on such a site (or in an email) that they would not put in a formal letter, be prepared to say in a face-to-face conversation or discuss in a public place.
   9. Any information published online can be accessed around the world within seconds and will be publicly available for all to see, and is not easy to delete/withdraw once published. The trust/school views any comment that is made on a social media site as made publicly, and that any inappropriate comment made, will be considered in the context of which it is made. Staff are advised to be mindful that nothing on a social media site is ‘private’ so comments made must still meet the standards of the role-specific code of conduct and other relevant policies.
   10. Staff may be accountable for actions outside of work, including making comments on social media sites, if that is contrary to any of trust/school policies, impacts on or compromises the staff member's ability to undertake their role, or undermines management decisions. Such behaviour would be investigated and may result in disciplinary action being taken, and could result in dismissal.
   11. When reaching decisions relating to potential disciplinary cases for breach of such a code, to the difficulty of staff members in ‘controlling their image’ all the time, and that manipulation by others is extremely easy. Consideration would be given as to whether the ‘image’ had been created voluntarily by the member of staff.
   12. The school/trust views any comment that is made on social media to, potentially, have been made publicly. However, any inappropriate comment be considered in the context in which it is made. Members of staff should inform the headteacher if they consider any content shared on a social media site potentially conflicts with their role.
   13. Many staff will use social networking outside of work to keep in touch with family, friends or activity groups. There will clearly be occasions when contacts within these situations result in links between staff and pupils at a school (for example being ‘friends’ with a parent of a pupil). Staff should try to ensure that in such circumstances they can make a professional distinction between their role as a ‘friend’ outside work and their role within work.
   14. Whilst generic political discussion is not to be discouraged, staff must not participate in discussions that may bring the trust/school into disrepute and not give information or advice that they know to be contrary to trust/school policies or interests. Staff should not engage in chat which would embarrass, misrepresent or convey an unjust or unfavourable, impression of the trust/school or its business affairs, staffs, suppliers, pupils or their families. Staff should remember these sites are public forums.
   15. Any communications that staff make through social media must not:

* bring the trust/school into disrepute, for example by:
  + criticising, disagreeing or arguing with parents, colleagues or managers
  + making defamatory comments about individuals or other organisations/groups;
  + posting images that are inappropriate or links to inappropriate content;
* breach confidentiality, for example by:
  + referring to confidential information about an individual (such as a colleague or pupil) or the trust/school
* do anything that could be considered discriminatory against, or bullying or harassment of, any individual or group of individuals, and in contravention of trust/school policies, for example by:
  + making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation,  
    religion or belief or age;
  + using social media to bully another individual (such as the staff of the organisation), or posting images that are discriminatory or offensive or links to such content.
* take other action that impacts on the employee’s ability to do their job, for example by
  + online activity that is incompatible with the position they hold in the trust/school
  + any breach occurring inside or outside the workplace that is likely to affect the employee doing his/her work.
* contravene trust/school policies, for example;
  + the relevant code of conduct, the anti-bullying policy, or the equality & diversity policy.
  1. The trust/school strongly recommends to all staff that personal interactions on social media sites do not include any reference to your work.
  2. The above examples are not a definitive list of the misuse of social media but are examples to illustrate what misuse may look like.
  3. Staff should use common sense when posting items; think about the intended audience and the consequences of making unwise remarks about colleagues, pupils or the school and its wider stakeholders. No sensitive or confidential information relating to the trust/school must be revealed on social networking sites.
  4. Staff should be aware of the potential risks of communicating with ex-pupils in ways which may be considered as inappropriate – particularly if it could be shown that the adult-pupil relationship of trust had been breached.
  5. Staff should report any inappropriate contact from pupils or parents/carers to a member of Senior Leadership Team at the earliest opportunity to prevent situations from escalating.
  6. Staff are reminded that, as a safeguarding issue, they should always be careful about who they are ‘talking to’. It is very easy to hide identity in an on-line conversation.
  7. Staff are reminded that they have a responsibility to report any racist, sexist or other discriminatory comments they become aware of through postings or chat on such sites.
  8. In summary, staff are advised to safeguard themselves and their privacy when using social media sites. Areas of which to be mindful:
     1. Setting the privacy levels of personal sites
     2. Being aware of location-sharing services
     3. Opting out of public listings on social networking sites
     4. Logging out of accounts after use
     5. Keeping passwords safe and confidential
     6. Not representing personal views as those of the school.
  9. Staff should be aware that all comments made through social media must meet the standards of the relevant legislation and regulations, including data protection legislation (GDPR 2018) and the expectations of staff conduct as expressed in the school’s policies for the management of Human Resources.

1. Access to social media at work, for personal use
   1. Staff are not allowed to access social media websites for personal use from the school’s computers or devices or their own personal devices (e.g. mobile phones and wearable technology such as smart watches) during working hours (contact time for teachers and teaching assistants), and they must not be left running “in the background”, whilst at work.
   2. Leaving social media sites ‘running’ constantly in work time is considered to be a breach of the acceptable use policy, and would be considered to be using school resources for personal use, in work time, and as such would be investigated under the Disciplinary Procedure. These provisions also apply to personal computers and mobile devices.
2. School social media accounts
   1. Staff who have not been authorised to manage, or post to, a ONE Academy Trust or school social media account (e.g. Twitter) must not access, or attempt to access the account.
   2. Those who are authorised to manage the account must ensure they abide by the guidelines in this policy and any specific policy related to the account, at all times.
   3. Members of staff who follow and/or like the trust or school official social media channels are advised to use dedicated professional accounts, where possible, to avoid blurring professional boundaries.
3. Responding to online safety incidents and concerns
   1. All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
   2. All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
   3. Parents, carers and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure. We require staff, parents, carers and pupils to work in partnership to resolve online safety issues. After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required. Where there is suspicion that illegal activity has taken place, we will follow the local safeguarding procedures which will include contacting the police, calling either 101 about a concern, or 999 if there is immediate danger or risk of harm. If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL/*headteacher* will speak with 'Call Derbyshire'.

**Dealing with inappropriate references to the school or staff**

* 1. Staff and volunteers etc. who find that ‘friends’ have posted inappropriate material relating to themselves on a social media site, should consider asking them and the site to remove it. They should also consider informing the headteacher or CEO (as appropriate) if there is the potential for repercussions for the school/trust.
  2. If you find yourself the target of complaints or abuse on social networking sites you can take action yourself by using the mechanisms to report abusive activity. Most sites also provide some support for users who are subject to abuse. Again, it is advisable to let the headteacher/CEO know so you can benefit from their support.
  3. If you find inappropriate references to you or the school posted by parents, colleagues, pupils or other members of the community, it is very important that you report this to the headteacher/CEO as soon as possible. Do not attempt to address the situation yourself. The headteacher/CEO will then respond to the situation and ascertain your support needs.
  4. All staff have a professional duty to report any knowledge of colleagues posting inappropriate content on social media which would breach the guidance contained above.

1. **Working from home and remote access**
   1. Staff may need to access personal data about other staff and pupils when working remotely, including when managing online learning.
   2. Where possible staff will access personal data on either a secure cloud service or a server on the ONE Academy Trust IT network that is accessible through a virtual private network (VPN), so they do not need to keep any data on their devices
   3. Staff accessing the school’s ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school’s ICT facilities outside the school and take such precautions as the IT provider may require from time to time against importing viruses or compromising system security.
   4. Wherever possible, devices will be provided by the trust/school, so that appropriate security arrangements are in place. Whether using trust/school equipment or personal equipment, staff should ensure that:

* The device is password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
* Wherever possible the hard drive is encrypted - this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
* Make sure the device locks if left inactive for a period of time
* Avoid sharing personal devices you use for work purposes with family or friends
* Antivirus and anti-spyware software are kept up-to-date

1. **Virtual meetings** 
   1. Staff (including governance roles) working from home or unable to meet physically may make use of virtual meetings using apps such as Microsoft Teams. All users must be aware of safeguarding and data protection considerations when making use of these applications and ensure that:

* They are made aware of and follow specific security guidance related to the use of the chosen application
* They attend meetings with the webcam/video switched on where possible
* They prevent unauthorised individuals from overhearing conversations (for example, by using headphones)
* They are mindful of their surroundings and consider the privacy of the room, including, but not limited to, who or what is visible or audible in the background
* The meeting is not recorded unless permission is granted for the clerk/minute secretary alone to record the meeting to draw up the minutes. The recording will be handled in line with the UK General Data Protection Regulation (GDPR), and once it is no longer needed, the recording will be deleted.

1. **Remote learning**
   1. Each school's Remote Learning Policy sets out the protocols for periods of remote learning and using video conferencing facilities for delivering lessons and interacting with pupils and parents.
   2. All Remote Learning provision should be covered by an appropriate Risk Assessment.
   3. Parents/carers must agree to the conditions of use of the relevant software ('opt-in') e.g. Microsoft Teams, Class DoJo etc. in accordance with Data Protection Legislation.
   4. Remote learning will only take place using the school/trust approved systems. Staff will only use ONE Academy Trust managed or specific, approved professional accounts with learners and/or parents/carers.Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.
   5. Staff will only use ONE Academy Trust provided equipment and software for delivery of remote learning.
   6. All remote lessons will be formally timetabled. Online contact with learners and/or parents/carers will not take place outside of the operating times set by the headteacher.
   7. Live-streamed remote learning sessions will only be held with approval and agreement from the headteacher.
   8. Live-streamed remote learning sessions may be recorded with the consent of the headteacher and those taking part. Consent for recording and storage will be sought from parents as part of each school's Remote Learning provision. There must be a clear purpose for making the recording and this should be made clear to parents/participants (e.g. safeguarding considerations) and arrangements for storage (how the recording will be stored, length of time and access) must be specified in accordance with data protection legislation.
   9. Any personal data used by staff when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.
   10. A record of the length, time, date and attendance of any sessions held will be created. This will be stored securely as part of attendance records in line with the data protection policy. This is done automatically as part of MS Teams and does not need to be recorded or stored separately.

* 1. Appropriate privacy and safety settings will be used to manage access and interactions. This includes:
  + language filters
  + disabling/limiting chat
  + staff not permitting learners to share screens
  + keeping meeting IDs private
  + use of waiting rooms/lobbies or equivalent.
  1. When live streaming with pupils:

**I have read and understood <** **school/setting name> Video Conferencing and/or Live Communication Acceptable Use Policy (AUP).**

**Learner/Parent/Carer**

Child’s Name……………………………………………………………………………………………...

Class…………………………

Parent/Carers: ……………………………………………......................................................

Date (DDMMYY)………………………………………………...

**Staff**

Name: …………………………………………………………………………………………………

Date (DDMMYY)………………………………………………...

* contact will be made via school/setting provided email accounts and/or logins or via a parent/carer's account.
* staff will mute/disable learners’ videos and microphones as appropriate
  1. Live sessions will be made available between the teacher and a group of children to talk to staff and share achievements/issues with work. These may be recorded and stored on school equipment as protection for staff should there be an allegation of inappropriate behaviour. The staff member will always be the last to leave the meeting.
  2. Live 1:1 sessions with pupils will only take place with approval from the headteacher and parental agreement. A parent/carer is required to be present in the room.
  3. A pre-agreed invitation/email detailing the session expectations will be sent to those invited to attend. Access links should not be made public or shared by participants.
  4. Pupils are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.
  5. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom. All participants are expected to behave in-line with existing school/setting policies and expectations. This includes:
* appropriate language will be used by all attendees.
* staff will not take or record images for their personal use.
* staff and attendees will wear appropriate dress.
* ensuring backgrounds of videos are neutral (blurred if possible).
* ensuring that personal information and/or unsuitable personal items are not visible, either on-screen or in video backgrounds.
  1. Staff will remind attendees of behaviour expectations and how to report concerns at the beginning of the session.
  2. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to the headteacher.
  3. Inappropriate online behaviour will be responded to in line with the appropriate school policies. Sanctions for deliberate misuse may include:
* restricting/removing use
* contacting the police if a criminal offence has been committed.
  1. Any safeguarding concerns must be reported to the school Designated Safeguarding Lead, in line with the school's child protection and safeguarding policy.

22.22 A useful reference source for protocols for Remote Working is the: [DfE guidance on Safeguarding & Remote Education](https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19)

1. **Safeguarding**
   1. With the increased access of both pupils and staff to electronic communication, there is an increased chance of a disclosure being made to a member of staff through such a medium. Such a disclosure may be made outside normal working hours. The member of staff must follow the normal trust/school procedures for reporting a disclosure as soon as they access the disclosure. This is set out in the child protection and safeguarding policy.

*(A further useful reference source is the booklet “Guidance on Safer Working Practice for Adults Who Work with Children and Young People”)*

1. **Early Career Teachers**
   1. There can be particular issues for those new to the profession relating to the use of social network sites. It is likely that throughout their training period, they will have been regular users of such sites and have possibly been less concerned about the content of their ‘pages’ or the image they have presented of themselves. As part of their induction, they should be made aware of the issues raised above as a matter of priority and be advised to remove any material from such sites that may harm their new professional status. As many early career teachers maybe not much older than some of the pupils they will be working with, they must be made aware at a very early stage of the potential problems (including loss of job) that inappropriate comments and contact on social network sites (even if outside working hours) can cause.
2. **Monitoring and review**
   1. This policy and procedure will be reviewed annually or whenever a change in legislation or practice necessitates a review, whichever is sooner.

**Appendices**

**Employee guidance on the use of social media (summary)**

* Staff must be mindful that any online activities/comments made in a public domain, must be compatible with their position within the school/trust, and safeguard themselves in a professional capacity.
* Protect your own privacy. To ensure that your social network account does not compromise your professional position, ensure that your privacy settings are set correctly. Remember to upgrade access settings whenever the application/programme is upgraded.
* When setting up your profile online consider whether it is appropriate and prudent for you to include a photograph, or provide occupation, employer or work location details. Comments made outside work, within the arena of social media, do not remain private and so can have an effect on or have work-related implications. Therefore, comments made through social media, which you may intend to be “private” may still be in contravention of the one of the school/trust’s HR Policies. Once something is online, it can be copied and redistributed making it easy to lose control of. Presume everything you post online will be permanent and can be shared.
* Do not discuss work-related issues online, including conversations about pupils, parents, complaints, management or disparaging remarks about colleagues or the school. Even when anonymised, these are likely to be inappropriate. In addition, doing this in the presence of others may be deemed as bullying and/or harassment.
* Do not under any circumstances accept friend requests from a person you believe could be a ‘service user’ or may conflict with your employment.
* Be aware that other users may access your profile and if they find the information and/or images it contains offensive, make a complaint about you to the school as your employer.
* Ensure that any comments and/or images cannot be deemed defamatory, libelous or in breach of copyright legislation.
* You can take action if you find yourself the target of complaints or abuse on social networking sites. Most sites will include mechanisms to report abusive activity and provide support for users who are subject to abuse by others.
* If you do find inappropriate references and/or images of you posted by a ‘friend’ online you should contact them and the site to have the material removed. It is wise to alert your friends in advance to the implications for you, as a school employee, of posting material related to you.
* If you find inappropriate references to you posted by parents, colleagues, pupils or other members of the school community, report this to the headteacher.
* If you are very concerned about someone else's behaviour online, you should take steps to raise your concerns. If these are work related you should inform your manager/headteacher.
* Staff should also act in accordance with the all the school/trust’s human resources policies and Child Protection/ Safeguarding policies.
* Staff should not access social media sites or leave these running in the background during working hours (contact time for teachers and teaching assistants), on any of the school’s devices within their control.

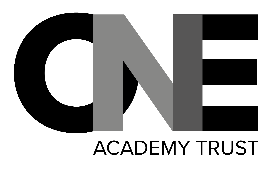
**Additional guidance for headteachers on the use of social media**

**Headteachers are responsible for:**

* Remaining familiar with this policy and the employee guidelines to using social media summarised in Appendix 1.
* Keeping up-to-date with relevant legislation and safeguarding issues regarding the use of social media.
* Ensuring staff and volunteers are made aware of the policy, guidelines and provided with appropriate training/briefing on induction and at regular intervals.
* Taking prompt action to stop any harassment or bullying they become aware of, whether a complaint has been raised or not, including taking steps to seek the prompt removal of any inappropriate material.
* Making parents and pupils aware of the implications of posting comments about the school and members of its community. Details should be included in the Home School Agreement and/or school brochure to indicate the appropriate means for parents of raising any concerns. It is advised that these documents also make reference to the potential implications of posting inappropriate comments about the school/staff/pupils/wider community members. The agreement will also warn against the unauthorised taking of photographs of staff and/or making sound recordings.
* Supporting employees who are the subject of abuse, through existing policies and procedures.
* Ensuring all complaints/allegations are dealt with fairly and consistently, and in accordance with other employment policies where appropriate.

**Headteachers are advised to:**

* Ensure staff are advised of this policy on appointment and discussion and elaboration is included during induction such that they are fully aware of its content.
* Remind staff on an annual basis of the guidance on use of social media.
* Ensure staff are aware of how to raise concerns
* Include in the relevant section of the Information and Communication Technology curriculum, advice for pupils on the safe use of social media, the restrictions on use of these media for contact with school staff and the implications of posting material on such sites.
* Provide guidance for parents in supporting their children’s safe use of social media
* Include in documents like the school brochure and home/school agreement, the school’s approach to the taking of photographs of pupils, by the school or by parents, and how these may be used. Seeking parents’ agreement at the outset and alerting them to potential pitfalls is likely to reduce issues of concern occurring. Parents may need to be made aware of the potential consequences of posting pictures on social media which include children other than their own, without parents’ permission.
* Ensure parents and pupils are made aware that the use of social media to make inappropriate comments about staff, other parents or pupils will be addressed by the school in the same way as if these remarks were made in person, in the public domain. Outline how such actions are likely to be damaging to the smooth running of the school and therefore the delivery to children.
* Respond quickly to those posting inappropriate comments. You may wish to issue a standard letter from the chair of governors asking them to contact the school/named person on a specific number. When following up, direct them to the appropriate processes for addressing issues or lodging complaints. Ensure the school’s actions demonstrate both that harassment will not be tolerated and that expressing concerns though appropriate channels will ensure they are taken seriously.



**Acceptable use of IT, the internet and electronic communication**

**VOLUNTEERS AND VISITORS**

**(who are provided access to the school's IT facilities)**

|  |  |
| --- | --- |
| **Name:** | |
| When using the school’s ICT facilities and accessing the internet in school, or outside the school on a work device, I will not:   * Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) * Use them in any way which could harm the school’s reputation * Access social networking sites or chat rooms * Use any improper language when communicating online, including in emails or other messaging services * Install any unauthorised software, or connect unauthorised hardware or devices to the school’s network * Share my password with others or log in to the school’s network using someone else’s details * Share confidential information about the school, its pupils or staff, or other members of the community * Access, modify or share data I’m not authorised to access, modify or share * Promote private businesses, unless that business is directly related to the school | |
| * I understand that the school will monitor the websites I visit and my use of the school’s ICT facilities and systems. * I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school’s data protection policy. * I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. * I will always use the school’s ICT systems and internet responsibly and ensure that pupils in my care do so too. | |
| **Signed:** | **Date:** |

Model policy for pupils & parents

Each school to adapt to suit their purposes

**Acceptable Use of IT, the internet and electronic communication**

**PUPILS & PARENTS**

At < insert name of school> we take the safety of our pupils both in and out of school very seriously.

Within school all children are taught about how to stay safe online and how to report incidents.

In Reception and KS1 this focuses on how to use tablets and computers, making sure that they are supervised and know how to ask for help if they need it. We also teach them about why we need to be careful when using the internet.

Insert as appropriate:

In KS2 we develop this further, building on the foundation of what they have learned in KS1. The children learn about how to use technology, the information they should and should not share, how to be safe online, how to report issues, and their online interactions with others.

Our Remote Learning provision, developed in response to the COVID-19 pandemic, may require some online interaction between pupils and parents at home and teachers providing lessons and guidance on learning.

<We provide email addresses for direct contact with teachers.>

Please could you read through the Parent section below and read through and discuss the Reception/KS1 or the KS2 section with your child to make sure they understand what it means.

Please note that because of your child attends < insert name of school>, it is an expectation that you and your child are agreeing to abide by the school's policies. Please see the home/school agreement for further information.

**Parents**

1. Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: <insert as appropriate>

* Our official Facebook page
* Our school Twitter account
* Email/text groups for parents (for school announcements and information)
* Our virtual learning platform

1. Parents/carers also set up independent channels to help them stay on top of what’s happening in their child’s class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).
2. When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

* Be respectful towards members of staff, and the school, at all times
* Be respectful of other parents/carers and children
* Direct any complaints or concerns through the school’s official channels, so they can be dealt with in line with the school’s complaints procedure

I will not:

* Use private groups, the school’s Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can’t improve or address issues if they aren’t raised in an appropriate way
* Use private groups, the school’s Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I’m aware of a specific behaviour issue or incident
* Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children’s parents/carers
* Seek to "friend" on social media staff working at the school.

1. I understand that if I am provided with access to a school learning platform where posting or commenting is enabled I will abide by any additional acceptable use requirements that are provided as a condition of use.
2. I understand that if I am provided with access to a live video link for the purposes of my child's remote learning or meetings with teaching staff, I will abide by any additional acceptable use requirements that are provided as a condition of use. For example:
   * I will not record or capture images of staff.
   * I will be respectful and behave appropriately at all times
   * I will report any concerns to the headteacher immediately
3. I understand that my child’s safe use of the internet and online technologies outside of school is my responsibility

**Pupils - Reception & KS1**

**This is how we stay safe when we use computers and the internet:**

* I will ask an adult if I want to use the computer
* I will only use activities that an adult says are ok
* I will take care of the computer and other equipment
* I will ask for help from an adult if I not sure what to do or I think I have done something wrong.
* I will tell an adult if I see something that upsets me on the screen
* I know that if I break the rules I might not be able to use a computer

**I understand these computer rules and will do my best to follow them**

**Pupils - KS2**

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

**For my own personal safety in school and at home:**

* I understand that the school will monitor my use of ICT in school.
* I will keep school usernames and passwords safe and secure. I will not share it. I will not use anyone else’s password (even with their permission).
* I will be aware of “stranger danger”, when I am communicating online.
* I will not share personal information about myself or others when online without telling an adult first (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, photos etc…)
* I will tell a trusted adult if anything I see online makes me feel uncomfortable or upset.
* I will never answer unpleasant, suggestive or bullying emails or messages and I will always report them to a teacher or parent. I know not to delete them straight away but show them to the person I have reported it to, as evidence.

**I understand that everyone has equal rights to use technology as a resource and:**

* I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission from a member of staff.
* I will not use the school systems or devices for on-line gaming or video broadcasting, unless I have permission from a member of staff.
* I will seek permission before I use a memory stick from home in a school computer.

**I will act as I expect others to act toward me:**

* I will respect other pupils work and property and I will not access, copy, remove or otherwise alter anyone else's files without the owner’s knowledge and permission.
* I will be polite and responsible when I communicate with others, I will not use inappropriate language and I appreciate that others may have different opinions.
* I will not take photographs or share pictures of anyone without their permission.

**I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:**

* I can bring a mobile phone into school with the headteacher’s permission and it will be kept in the school office. I will not bring any other personal devices into school.
* I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering /security systems in place to prevent access to such materials.
* I will immediately report any damage or faults involving equipment or software, however this may have happened.
* I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organization who sent the email.
* I will not install, or attempt to install or store, programmes of any type on any school device. I will not try to alter computer settings.
* I know that I am not allowed on personal e-mail, social networking sites or instant messaging in school. *The majority of these are filtered out by the school’s filtering system.*

**When using the internet for research or recreation, I understand that:**

* I should ensure that I have permission to use the original work of others in my own work.
* Where work is protected by copyright, I will not try to download copies (including music and videos)
* When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

**I understand that I am responsible for my actions, both in and out of school:**

* I understand that the schoolalso has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement, when I am out of school and where they involve my membership of the school community *(examples would be cyber-bullying another member of the school community, use of images or personal information of another member of the school community, posting threatening /offensive comments regarding another member of the school community).*
* I understand that if I fail to comply with this Acceptable Use Policy Agreement, I may be subject to disciplinary action. This may include:
  + loss of access to the school network/internet
  + contact with parents
  + exclusion
  + in the event of illegal activities - involvement of the police.

**MS Teams – Remote Learning Code of Conduct:**

I understand that by joining the sessions I agree to follow the code of conduct outlined below:

* I understand that while online, I must behave the same way as I am expected to behave in school.
* I will make sure that my communication online is always supportive of my learning and the learning and wellbeing of others. I will communicate in a respectful way at all times.
* During live online sessions, my parent/carer will be near me (in the room or a nearby room with the door open).
* I will end sessions when the teacher tells me to do so.
* When taking part in an online session I will make sure that my environment is quiet and free from distractions, the background is appropriate (check what is visible behind you).
* I will ensure that I am suitably dressed (fully dressed and not in pyjamas!).
* I will remain attentive.
* I will sign into MS Teams every day to help ensure that I keep on track with my learning.
* I will not take photos of my screen or record online interactions.
* At the end of live meetings my teacher will ask me to ‘hang up’ before closing the meeting. I will do this promptly as directed by my teacher.
* I understand that online sessions will be recorded by my teacher but that the recordings will not be made public.
* I understand that should I fail to follow this Code of Conduct, my teacher will remove me and contact my parents.

Remember with social media, when you type something it's always there and you can't take it back. So be careful of what you say and write.

**Part 1 - Agreement**

One copy for parent/carer and one copy to be retained in school

|  |
| --- |
| **This agreement is between:**  [*Insert name of school*] (“the school”) AND[*name of parent*] (“the parent” and “I”)  and governs the use and care of devices assigned to the parent’s child (the “pupil”). This agreement covers the from the date the device is issued through to the return date of the device to the school.  All issued equipment shall remain the sole property of the school and is governed by the school’s policies.  The school is lending the pupil [a laptop/tablet, etc] (“the equipment”) for the purpose of [doing schoolwork from home/special project, etc] period  This agreement sets the conditions for taking a [*Insert name of school*] [laptop/tablet] (“the equipment”) home.  I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the pupil will adhere to the terms of loan. |

1. **Damage/loss** 
   1. By signing this agreement, I agree to take full responsibility for the loan equipment issued to the pupil and I have read or heard this agreement read aloud and understand the conditions of the agreement.
   2. I understand that I and the pupil are responsible for the equipment at all times whether on the school’s property or not.
   3. If the equipment is damaged, lost or stolen, I will immediately inform the headteacher and I acknowledge that **I am responsible for the reasonable costs requested by the school to repair or replace the equipment.** If the equipment is stolen, I will also immediately inform the police.
   4. I agree to keep the equipment in good condition and to return it to the school on their demand from the school in the same condition.
   5. I will not leave the equipment unsupervised in unsecured areas.
   6. If the equipment is damaged, lost or stolen, and your child is eligible for the pupil premium, contact thev headteacher.
   7. I will make sure my child takes the following measures to protect the device:
      1. Keeps the device in a secure place when not in use
      2. Does not leave the device in a car or on show at home
      3. Does not eat or drink around the device
      4. Does not lend the device to siblings or friends
      5. Does not leave the equipment unsupervised in unsecured areas
2. **Unacceptable use** 
   1. I accept that there are no parental controls installed on this device and that I accept sole responsibility for monitoring any content that my child accesses.
   2. I am aware that the school monitors the pupil’s activity on this device.
   3. I agree that my child will not carry out any activity that constitutes ‘unacceptable use’. This includes, but is not limited to the following:
      1. Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
      2. Any illegal conduct, or statements which are deemed to be advocating illegal activity
      3. Activity which defames or disparages the school, or risks bringing the school into disrepute
      4. Causing intentional damage to ICT facilities or materials
      5. Using inappropriate or offensive language
   4. My child will abide by the school's pupil IT policy [*Insert name of policy, code of conduct as appropriate* ]
   5. I accept that the school will sanction the pupil, in line with our behaviour/discipline policy, if the pupil engages in any of the above at any time.
3. **Personal use**

I agree that the pupil will only use this device for educational purposes and **not for personal use** and will not loan the equipment to any other person.

1. **Data protection**

I agree to take the following measures to keep the data on the device protected.

* 1. Keep the equipment password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
  2. Make sure my child locks the equipment if it’s left inactive for a period of time
  3. Do not share the equipment among family or friends
  4. Update antivirus and anti-spyware software as required
  5. Install the latest updates to operating systems, as prompted
  6. If I need help doing any of the above, I will contact the school.

1. **Return date**
   1. I will return the device in its original condition to the school office within 5 working days of being requested to do so.
   2. I will ensure the return of the equipment to the school if the pupil no longer attends the school.
2. By accepting this loan device, you are affirming that your child will engage with Remote Learning from home. If our monitoring shows that your child is not using the device loaned to engage wth remote learning, the school will request its return.
3. **Consent**

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

| **Pupil’s full name:** |  |
| --- | --- |
| **Parent’s full name** |  |
| **Parent’s signature** |  |

**Device Loan Agreement for Pupils**

**Part 2 - Record of loan**

To be filled out by staff signing out/receiving the equipment. **To be retained in school.**

| **Details of pupil** | | | | |
| --- | --- | --- | --- | --- |
| Pupil Name | |  | | |
| Year & Class | |  | | |
| Parent’s Name (who signed the agreement): | |  | | |
| **Loan details** | | | | |
| Date of Issue |  | | | |
| **Equipment Details** | | | | |
| Type |  | | | |
| Make |  | | | |
| Model |  | | | |
| Serial Number |  | | | |
| Replacement Value |  | | | |
| Equipment Condition |  | | | |
| **Accessory Details** | | | | |
| **Description** | | | | **Quantity** |
|  | | | |  |
| **Equipment Return** | | | | |
| Date Returned | | |  | |
| Equipment returned in original condition? | | | **Yes No** | |
| **Comments if not in the original condition:** | | | | |