Cundall Manor School

Information Technology and Digital Safety Policy

Created	August 2023
Next Review	August 2024
Headmaster	Chris James-Roll
Deputy Head Pastoral	Clare Stovin
IT Manager	Adam Fosker
Business Manager	Laura Taylor

Contents

Schedule for monitoring and review

The policy will be reviewed yearly by the governing body of the school.

The school will monitor the impact of the policy using: -

- Logs of reported incidents
- Monitoring logs of internet activity/filtering
- Internal monitoring of network activity

Scope of the policy

This policy applies to all staff and students within the school who have access to and are users of the school's digital technology. This policy should be read in conjunction with the school safeguarding policy.

The Education and Inspections Act 2006 empowers Senior Leaders to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Serious Disciplinary Policy and Procedures.

Information Technology is commonly abbreviated to IT. This is all the infrastructure, the physical hardware through to the operating software used to power computing systems. IT can include computers, phone systems and email accounts – it also incorporates the systems required to run these services, such as software, antivirus, security and personnel.

Digital is how you utilise information technology to communicate and build relationships with staff, students, parents and other stakeholders online. Digital can include websites, apps, social media, e-mail marketing and online advertising.

Responsibilities

Governors

Governors are responsible for the approval of the policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of Safeguarding Governor.

The governing body will review the standards and discuss with IT staff and service providers what more needs to be done to support schools and colleges in meeting standards.

Senior Leadership Team

- The headmaster has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Designated Safeguarding Lead (DSL).
- The headmaster and the DSL should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headmaster is responsible for ensuring that the DSL and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- The headmaster will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular updates from the Designated Safeguarding Lead regarding incidents.
- The headmaster will assemble a small group of senior staff whom will review and test the integrity of the school system Termly by attempting to access inappropriate content using approved and non-approved user profiles. The group will notify the headmaster and IT Manager beforehand and record their actions, findings and recommendations.

Information Technology Manager

The IT Manager must ensure: -

- The school's technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets required online safety technical requirements.
- That users may only access the networks and devices through properly enforced password protection.
- Filtering is applied and updated on a regular basis.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network is regularly monitored in order that any misuse/attempted misuse can be reported to the DSL for investigation and appropriate action.
- That monitoring software / systems are implemented and updated as agreed in school policies.

All Staff

Are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school policies.
- They have read, understood and agreed to all school policies.
- They report any suspected misuse or problem to the Designated Safeguarding Lead for investigation and appropriate action.
- All digital communications with pupils, parents / carers should be on a professional level and only carried out using official school systems .
- Online safety issues are embedded in all aspects of the curriculum and other activities .
- Pupils understand and follow the Online Safety Policy and acceptable use policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use, and that processes are in place for dealing with any unsuitable material that is found in internet searches .

Designated Safeguarding Lead (DSL)

The DSL is trained in Online Safety issues and is aware of the potential for serious child protection or safeguarding issues arising from:

- Sharing of personal data.

- Access to illegal/inappropriate materials.
- Inappropriate on-line contact with adults/strangers.
- Potential or actual incidents of grooming.
- Online-bullying.

The DSL will ensure all staff have appropriate training applicable to their roles in relation to filtering and monitoring

Pupils

- Are responsible for using the school digital technology systems in accordance with this acceptable use policy.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold
- copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate
- materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital
- cameras. They should also know and understand policies on the taking and using of images
- and on online-bullying.
- Should understand the importance of adopting good online safety practice when using digital
- technologies out of school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' presentations, the newsletter, letters and the parent portal. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of: -

- Digital and video images taken at school events.
- Access the parent portal.
- Their children's personal devices in the school.

Appendix 1: Acceptable Use Policy - Staff

The school recognises that digital technology and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practise good online safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

Staff at Cundall Manor School are expected to be professional and exhibit good behaviour in their use of the school network at all times. Ultimately Cundall Manor School owns the computer network and sets both the guidelines for its use and sanctions for misuse. Staff are expected to respect the equipment provided by school and to abide by the various policies concerning the use of computers at Cundall Manor School. This applies to all staff working in the school whether paid or unpaid, whatever their position, role or responsibilities and includes employees, governors, supply staff, casual workers, contractors, work experience students and volunteers.

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

Staff should expect that violation of the rules below will result in a ban on computer and network use and may include other disciplinary action in accordance with the School's Discipline Procedure Policy. When applicable, the Police or local authorities may be involved.

Principles

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

The same principles apply when using all platforms and means of access to online activity whilst at work.

At Cundall Manor School, we are: -

- Responsible for our behaviour
- Aware how we interact with others
- Safe with the materials we use and create

Personal Safety

1.1. Staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for education, personal and recreational use.

1.2. Cundall Manor School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

1.3. This policy is intended to ensure that staff are protected from potential risk in their use of ICT in their everyday environment.

1.4. Staff understand that Cundall Manor School can monitor use of the systems, devices and digital communications if there is reason to suspect inappropriate use whilst performing school duties or functions, at the headmaster's discretion. School does not routinely look at staff members' internet history.

1.5. Staff will keep their username and password safe and secure for any online account – staff will not share it, nor will they try to use any other person's username and password. Staff

understand that they should not write down or store a password where it is possible that someone may steal it.

1.6. Staff should not give their personal contact details to students, including email addresses, home or mobile telephone numbers, unless the need to do so is agreed with the Designated Safeguarding Lead and parents, guardians or carers.

1.7. Do not leave any computer unattended with an open (logged on) session. This also applies to remote sessions on portable devices or from home. If staff need to leave a computer briefly, they should lock the session. For longer periods unattended, staff should log off from the computer.

1.8. Staff will immediately report any illegal, inappropriate or harmful material or incident they become aware of to the Designated Safeguarding Lead (DSL) or a nominated safeguarding officer.

Interacting with others

1.9. Staff will not attempt to make large downloads or uploads that might take up internet capacity
and prevent other users from being able to carry out their work.

1.10. Staff will not engage in any online activity that may compromise their professional responsibilities.

1.11. Staff will not access, copy or otherwise alter any other user's files, without their express permission.

1.12. Staff will be polite and professional when communicating with others and adhere to the email etiquette policy; they will not use strong, aggressive or inappropriate language and will appreciate that others may have different opinions.

1.13. Staff will ensure that when they take and/or publish images of others, they will do so with permission and in accordance with the school's policy of the use of digital/video images. Where images are published (e.g., on the school website or newsletter) it will not be possible to identify by full name, or other personal information, those pupils who are featured.

1.14. Staff know that it is a criminal offence to possess, manufacture or distribute indecent images and videos of children (under the age of 18).

1.15. Staff will only use chat and social networking sites in school in accordance with the school's policies and the Staff Code of Conduct.

1.16. Staff will only communicate in a professional capacity with students and parents using official school systems. Any such communication will be professional in tone and manner. Staff should be made aware of the risks attached to using their personal email addresses/mobile phones/social networking sites for such communications.

1.17. Cundall Manor School staff are encouraged to activate their own 'Out of Office' message when away from school for more than one working day. This message can also be activated remotely from Outlook Web Access if a member of staff is ill.

Maintaining security and integrity

1.18. Access to educational computing facilities is managed by the Digital Services and Data Team. Equipment is allocated to individuals and/or departments by Cundall Manor School Digital Services and Data Team, and the use of any of Cundall Manor School computing facilities is at the discretion of the school.

1.19. The Computing facilities are owned by Cundall Manor School and software and/or data developed or created (for whatever reason) on that equipment remain in all respects the property of Cundall Manor School. The Patents Act 1977 and the Copyright, Designs and Patents Act 1988 provide for the Intellectual Property Rights (IPR) in that work created by an employee in the course of his/her employment is vested automatically to the employer.

1.20. Desktop PCs and school owned laptops are a critical asset to Cundall Manor School and must be managed carefully to maintain security, data integrity and efficiency. Users must never install software on or modify the hardware of any Cundall Manor School owned device without the written permission of the Digital Services and Data Team.

1.21. Laptop PCs and tablets are at high risk from loss or theft and require additional security protection, including encryption of hard disk drives where possible. All reasonable precautions must be taken to ensure that such hardware is stored securely. Also, to protect the integrity of Cundall Manor School systems and data procedures, passwords or authentication devices for gaining remote access to Cundall Manor School systems must not be stored with the computer. This includes the saving of passwords into remote access software. If your Laptop, PC or tablet is lost or stolen, the Digital Services and Data Team must be notified as soon as possible and a report made to the Police and the School Manager.

1.22. Loan equipment is similar to that for laptops and tablets. Most loan equipment is highly portable and attractive to thieves. Users who borrow loan equipment bear the responsibility for its care. Loan equipment should be concealed and stored securely when not in use. If loan equipment is stolen or lost, the Digital Services and Data Team must be notified as soon as possible and a report made to the Police and the School Manager.

1.23. Only software properly approved by the Digital Services and Data Team prior to purchase or download may be used on Cundall Manor School hardware. If a member of staff is unsure about whether they can install additional apps, they should in the first instance check with the IT Service Desk prior to installation. Non-standard or unauthorised software can cause problems with the stability of computing hardware. The copying and use of software without the licensor's permission is illegal. Cundall Manor School has licences to provide certain software titles to staff for use on their own hardware whilst employed at Cundall Manor School. When employment ceases the software must be removed.

1.24. Whilst it is the user's responsibility to take reasonable care over the configuration of their computer hardware, it is possible for software to be installed on a machine without the full comprehension of the user. Users discovering software that has been installed in an unsolicited manner must contact the Digital Services and Data Team who will assist in resolving any issues.

1.25. Staff will not disable or cause any damage to school equipment or the equipment belonging to others.

1.26. Staff understand the risks and will not try to upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others, nor will they use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

1.27. Staff will promptly report any damage or faults involving equipment or software; however this may have happened.

1.28. Staff will not open any hyperlinks in emails or any attachments to emails, unless they know and trust the person/organisation who sent the email, or if staff have concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes). If a staff member suspects that they have a virus, Trojan or ransom ware infection on their PC/laptop, they should shut the device down immediately and remove it from the wired and wireless network before seeking urgent assistance from the IT Service Desk.

1.29. Staff will ensure that their data is regularly backed up. Note that key data on the school Network and Google Drive are protected by regular automatic back-ups.

1.30. While staff may wish to use personal devices to check school accounts, such as email accounts (e.g., via email apps, or through a web browser), staff must not download any school data - including but not limited to: staff or pupil personal data; school or business data – to any device not issued by the school (for example, staff must not download any attachments or documents accessed through links, if accessing school email though a personal device).

1.31. Staff must not set up offline files or file synchronisation for school systems (e.g., email or Google Drive), on any non-school device.

1.32. Staff will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. Staff will not try to use any programmes or software that might allow them to bypass the filtering and security systems in place to prevent access to such materials.

1.33. Staff will not attempt to use any removeable storage device with school computers unless authorised by the IT the Digital Services and Data Team, such as USB memory sticks.

Responsibility for behaviour

1.34. The use of personal devices, wirelessly connected to the network, is allowed by all members of staff, however, all contents of this policy still apply. Do not use wired connections from personal devices to the network.

1.35. Staff understand that Cundall Manor School also has the right to take action against them if they are involved in incidents of inappropriate behaviour, that are covered in this agreement, when they are out of school and where they involve their membership to the school community (examples would be online bullying, use of images or personal information).

1.36. Staff understand that the data protection policy requires that any staff or student data to which they have access will be kept private and confidential, except when it is deemed necessary that they are required by law or by school policy to disclose such information to an appropriate authority.

1.37. Staff should ensure that their activity online is not defamatory and does not bring the school's name into disrepute, e.g., making defamatory comments about individuals, other organisations or groups, Cundall Manor School; or posting images that are inappropriate, links to inappropriate content or using inappropriate language.

1.38. Staff understand that if they fail to comply with this Acceptable Use Policy Agreement, they may be subject to disciplinary action. This may include amongst other potential measures the loss of access to the school network/internet, suspensions, and in the event of illegal activities involvement of the Police.

Use of Digital and Video Images

1.39. Staff understand the primary purpose of having their portable device at school is educational, irrespective of whether the device is school owned or personal.

1.40. Staff need to be aware of the risks associated with publishing digital images on the internet. Those images may provide an avenue for online bullying to take place; digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

1.41. In accordance with guidance from the Information Commissioner's Office, parents/guardians are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/guardians' comment on any activities involving other pupils in the digital/video images.

1.42. Staff are allowed to use school cameras and devices to record pupils' learning and attainment and any images should be appropriately stored solely on the school network and are not to be removed from the premises unless authorised and having been considered for appropriate use. In the event of images taken on tablet or other portable devices, or away from school, these should be uploaded to the appropriate school system and then deleted from the device at the first opportunity.

1.43. Staff who work in a one-to-one situation with students should be mindful when taking photographs; this should be relevant and appropriate to the needs of the child.

1.44. Video, audio and photographic recording must never take place without the consent of student(s) and teacher(s). Consent must be explicit, not implied.

1.45. Permission must be sought for the capture of images in areas which may be deemed to be sensitive, e.g., swimming pool. Staff should at all times ensure that all images they take or commission to be taken are wholly appropriate. Where an image inadvertently contains something which may be viewed as inappropriate, e.g., an unfortunate camera angle, this should be taken to the DSL immediately in a spirit of transparency so that this may be addressed immediately.

1.46. The use of personal devices to record or photograph pupils should be avoided if at all possible. If an image is taken using a personal device, the data must be downloaded onto the School network as soon as is possible and then deleted from the device and any other personal storage locations, including any backup. This should happen before taking the personal device home.

1.47. Photographs published on the website or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Use of personally owned devices

1.48. Staff must not connect any personal device to the wired network.

1.49. Staff may connect personal devices to the Cundall Manor School Guest WiFi network. However, those devices are subject to the same restrictions as any other device connected to the network and their use will be monitored as with school owned devices.

1.50. Staff personal devices are brought into school entirely at the risk of the owner and the decision to bring the device in to the school lies with the member of staff as does the liability for any loss or damage resulting from the use of the device in school.

1.51. Users are responsible for keeping their personal devices up to date through software, security and application updates. The device is virus protected and should not be capable of passing on infections to the network. Devices which do compromise the network will be blocked and the associated user account disabled.

1.52. The school accepts no responsibility or liability in respect of lost, stolen or damaged personal devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home).

1.53. The school accepts no responsibility for any malfunction of a personal device due to changes made to the device while on the school network or whilst resolving any connectivity issues.

1.54. The school recommends that personal devices are made easily identifiable and have a protective case to help secure them as the devices are moved around school.

1.55. Passcodes or PINs must be set on personal devices to aid security.

1.56. The school is not responsible for the day-to-day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.

1.57. Social media and messaging should only be used in compliance with the Staff Code of Conduct, and never for sending personal messages to students.

1.58. Students are not to use staff owned devices.

Managing emerging technologies

1.59. Technology is progressing rapidly and new technologies are emerging all the time. The school will risk assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have.

1.60. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for taking advantage of and dealing with new technological developments.

Staff Acceptable Use Agreement Form

1.61. All staff members are required to agree to the acceptable use policy as an intrinsic and necessary part of their employment at the school.

1.62. All staff members provide this consent electronically on an annual basis. By electronically consenting to the Staff AUP, staff members indicate that they have read, understood and agree to the Staff Acceptable Use Policy.

Appendix 2: Acceptable Use Policy - Students (Reception to Year 4)

Introduction

Using computers and tablets is a part of everyday life inside and outside school. They can help support your studying in school in exciting ways. All children should be able to use computers, tablets, and the internet safely.

Your Class Teacher will review this form with you, and if you have any questions you should talk to your Class Teacher and parents about them.

How we stay safe when we use computers

1. The school monitors what I do when I am using a school computer or tablet, and my parent/guardian may be contacted if a member of school staff is concerned about my safety or behaviour.
2. I will ask a teacher or suitable adult if I want to use the computers or tablets.
3. I will only use activities that a teacher or suitable adult has told or allowed me to use.
4. I will take care of the computer and other equipment.
5. I will only send teachers emails from my school email address.
6. I will not tell other people my ICT password.
7. When I am using a computer or tablet, I will not give out personal details, such as: my name, my phone number; or my home address.
8. I will not spoil or delete anyone's work.
9. I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
10. I will never be unkind or rude.
11. I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.
12. I know that some people online may lie about who they are and that some of the information on the web is not true.
13. I will be careful about who and what I believe, and will speak to a teacher if I am worried.
14. I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
15. I will tell my teacher or parent if something makes me worried or uncomfortable, or if I believe that someone is being bullied online.
16. I will shut the screen and then immediately tell a teacher or suitable adult if I see something that upsets me on the screen.
17. I know that if I break the rules, I might not be allowed to use a computer or tablet.
18. I will not attempt to bypass any systems put in place by the school to keep me safe, such as the firewall or anti-virus.

Appendix 3: Acceptable Use Policy - Students (Year 5 to Thornton)

Introduction

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

All students from Year 5 onwards bring in their own Chromebook to use within the school. It is the pupils' responsibility to look after this device, bring it to lessons, and ensure it is charged and ready for use when in school. Students must not log into a Chromebook as any account except their @cundallmanor.com one while on the school site.

This Acceptable Use Policy is intended to ensure that: -

- Cundall Manor School pupils will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- Cundall Manor School systems and users are: protected from accidental or deliberate misuse that could put the security of the systems at risk; and will have good access to digital technologies to enhance their learning and will, in return, we expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

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

Personal Safety

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc).
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

Equal rights to use technology as a resource

- 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.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, filesharing.
- I will not use the school systems for video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

Acting as I expect others to act toward me

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

Security and Integrity

- 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 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, software, proxy servers or virtual private networks (VPNs) that might allow me to bypass the filtering, monitoring and security systems in place to prevent access to such materials. If I notice I am able to access material which would not be deemed suitable in a school, I will immediately notify my teacher.
- 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/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with explicit permission and at the times that are allowed.

Using the internet for research or recreation

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not 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.

Responsible for my actions, both in and out of school

- I understand that the school also 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, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include: loss of access to the school network, and the internet while in school; detentions; exclusions; contact with parents; and, in the event of illegal activities, pupils should expect that the school would involve the police.

Every year, when the policy has been updated, you will go through this policy with your Form Tutor or Head of Year. If you are not happy with any aspect of this Acceptable Use Agreement, please speak with your Form Tutor or Head of Phase in the first instance and before your first log on to the School System, and any first log on following an update to this Acceptable Use Agreement. If you do not agree to abide by this Acceptable Use Agreement, access will not be granted to school systems and devices.

Appendix 4: E-mail Etiquette Policy

In order to promote effective communication and maintain professionalism in our email correspondence, we are implementing an Email Etiquette Policy which will form part of the Acceptable Usage Policy. This policy outlines the best practices and guidelines to follow when using email as a means of communication within School. By adhering to these guidelines, we can enhance clarity, efficiency, and mutual respect in our email exchanges.

1. Use clear and concise subject lines:
    - Choose subject lines that accurately reflect the content of the email.
    - Keep subject lines brief and informative to help recipients prioritize and search for emails effectively.
2. Maintain a professional tone:
    - Use a respectful and courteous tone in all email communications.
    - Avoid using overly informal language, slang, or jargon that may be unfamiliar to the recipient.
    - Double-check grammar, spelling, and punctuation to ensure clarity and professionalism.
    - Do not use emojis
3. Consider the recipient's time and inbox:
    - Before sending an email, consider whether it is necessary or if the information could be conveyed through alternative means. For example, face to face
    - Keep emails concise and to the point, avoiding unnecessary details or excessive content.
    - Use proper formatting (paragraphs, bullet points) to make the email easier to read and understand.
4. Reply promptly:
    - Aim to respond to emails within a reasonable timeframe, or as soon as practicable.
    - If you require more time to gather information or provide a thorough response, acknowledge receipt of the email and provide an estimated timeframe for your response.
5. Use appropriate language and tone:
    - Never use offensive, divisive or discriminatory language in emails.
    - Be mindful of cultural and social differences that may impact interpretations of tone or humour.
    - Assume positive intent when reading emails and avoid responding defensively.
6. Use a professional email signature:
    - Include your full name, job title, and contact information in your email signature.
7. Respect confidentiality and privacy:
    - Do not forward or share emails or their contents without permission from the sender, unless it is necessary for work-related purposes.
    - Be cautious when replying to or forwarding emails to ensure that confidential or sensitive information is not inadvertently shared with unintended recipients.
8. Think before forwarding or using "Reply All":
    - Ensure that forwarding or replying to all is appropriate for the content being shared.
    - Remove any unnecessary email threads or unrelated content when forwarding or replying to maintain clarity.

- Use the "Reply All" function only when necessary for all recipients to be aware of your response.
- Consider whether a reply is relevant to all recipients or if it can be directed to specific individuals. It should be a rare occurrence to minimise unnecessary email traffic

9. Properly manage attachments:
    - Only include attachments when necessary and ensure they are relevant to the email content.
    - Compress large files, when possible, to avoid overwhelming recipients' inboxes.
    - Never open attachments or links from unknown senders. Be aware of scams and viruses before sending on to others.
10. Employer data
    - Emails sent and received using School email accounts are the property of the school, can be monitored and searched. Email content is disclosable in a subject access request (SAR) and email users should be mindful of their email content and these guidelines.

Effective communication is key to our success as a School. By adhering to this Email Etiquette Policy, we can promote professionalism and clarity and prevent offence and upset in our email correspondences.

Appendix 5: Cyber Security

A cybersecurity incident can have a major impact on any organisation for extended periods of time. For a school, this can range from minor reputational damage and the cost of restoring systems from existing backups, to major incidents such as losing student work or access to learning platforms and safeguarding systems, which could lead to data-protection fines or even failing an inspection.

This Cybersecurity Policy outlines Cundall Manor School's guidelines and security provisions which are there to protect our systems, services and data in the event of a cyberattack.

Appendix 1 of this policy, the Staff Acceptable Use Policy, also contains information relating to Cyber Security.

Scope

This policy applies to all Cundall Manor School staff, contractors, volunteers and anyone else granted permanent or temporary access to our systems and hardware. It also covers the physical and technical elements that are used to deliver IT services for the school.

Physical Security

Cundall Manor School will ensure there is appropriate physical security and environmental controls protecting access to its IT Systems, including but not limited to air conditioning, lockable cabinets, and secure server/communications rooms.

User Accounts

Users are responsible for the security of their own accounts. If at any time they believe their credentials may have been compromised, for example after a phishing scam, they must change their password and inform the IT and Data Services Team as soon as possible. Personal accounts should not be used for work purposes. Cundall Manor School will implement multi-factor authentication where it is practicable to do so.

Data Backups

Data stored onsite on the physical hosts and in Google Workspace is backed up daily offsite to Acronis. There is a 1-month data retention policy in place.

Staff Leavers

Cundall Manor School utilises Salamander to disable Active Directory, 365 and Google Workspace accounts, this will happen the night of the user being made a leaver in the Schools MIS.

Training

Cundall Manor School recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. It will integrate regular Cybersecurity training into Inset days, provide more specialist training to staff responsible for maintaining IT systems and promote a "No Blame" culture towards individuals who may fall victim to sophisticated scams.

System Security

The IT and Data Services Team will build security principles into the design of IT services for Cundall Manor School.

- Security patching – network hardware, operating systems and software.
- Pro-actively plan for the replacement of network hardware, operating systems and software before vendors stop providing security support for them.
- Actively manage anti-virus systems.

- Actively manage backups.
- Regularly review and update security controls that are available with existing systems.
- Segregate wireless networks used for visitors' & staff personal devices from school systems.
- Review the security risk of new systems or projects.

File Permissions and Sharing

Cundall Manor School recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a date breach users are required to:

- Consider if an email could be a phishing email or that a colleague's account could be 'hacked'. If something does not feel right check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites.
- Wherever possible, keeping Cundall Manor School's files on school systems.
- Not share any specific school data outside of the school systems – including but not limited to student data, parent data and staff data.
- Not send school files to personal accounts.
- Verifying the recipient of data prior to sending.
- Use file encryption where possible, sending passwords/keys via alternative communication channels.
- Alert the DPO to any breaches, malicious activity or suspected scams.