ICT and Acceptable Use Policy (Primary School Version)

Newbury Academy Trust

May 2020

(Updated January 2021 – Pending Approval)

ICT and Acceptable Use Policy

Appendices:

ICT and Acceptable Use Policy

1. Introduction and Aims

"Academy" and "Academy Trust" refer to Newbury Academy Trust, Love Lane, Newbury, Berkshire, RG14 2DU. School refers to one of the three schools within the Newbury Academy Trust, Trinity School, Love Lane, Newbury, Berkshire, RG14 2DU; Fir Tree School, Fir Tree Lane, Newbury, Berkshire, RG14 2RA; Speenhamland School, Pelican Lane, Newbury, Berkshire, RG14 1NU.

The term Governor refers to both Board of Trustees and Local Governing Body Governors.

ICT is an integral part of the way our school works, and is a critical resource for students, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors;
- Establish clear expectations for the way all members of the school community engage with each other online;
- Support the school's policy on data protection, online safety and safeguarding;
- Prevent disruption to the school through the misuse, or attempted misuse of ICT systems;
- Support the school in teaching pupils safe and effective internet and ICT use.

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our Disciplinary policy and Behaviour and Discipline policy.

2. Relevant Legislation and Guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018;
- The General Data Protection Regulation;
- Computer Misuse Act 1990;
- Human Rights Act 1998;
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000;
- Education Act 2011;
- Freedom of Information Act 2000;

- The Education and Inspections Act 2006;
- Keeping Children Safe in Education 2019;
- Searching, screening and confiscation: advice for schools.

3. Definitions

"ICT facilities": includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, printers, scanners, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service.

"Users": anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

"Personal use": any use or activity not directly related to the users' employment, study or purpose.

"Authorised personnel": employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities.

"Materials": files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

4. Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the School's ICT facilities:

- Using the school's ICT facilities to breach intellectual property rights or copyright;
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination;
- Breaching the school's policies or procedures;
- Any illegal conduct, or statements which are deemed to be advocating illegal activity;
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate;
- Activity which defames or disparages the school, or risks bringing the school into disrepute;
- Sharing confidential information about the school, its pupils, or other members of the school community;
- Connecting any device to the school's ICT network without approval from authorised personnel (the Trust Business Manager);

- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data;
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel;
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities;
- Causing intentional damage to ICT facilities;
- Removing letters on keyboards, scratching screens or defacing IT facilities.
- Removing, deleting or disposing of ICT equipment, systems, programmes or information without permission by authorised personnel;
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation;
- Using inappropriate or offensive language;
- Promoting a private business, unless that business is directly related to the school;
- Using websites or mechanisms to bypass the school's filtering mechanisms;

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Associate Headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1. Exceptions from Unacceptable Use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Associate Headteacher's discretion. This approval should be sought from the Associate Headteacher by email documenting the reasons and nature of the use.

4.2. Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on behaviour, staff discipline and staff code of conduct.

Copies of all policies can be found on the School and Trust website, on Firefly and shared drives.

5. Staff (including governors, volunteers, and contractors)

5.1. Access to School ICT Facilities and Materials:

The Trust's Network Manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices;
- Access permissions for certain programmes or files.

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Trust Network Manager by email to itsupport@newburyacademytrust.org.

All staff, pupils, governors, volunteers and visitors will sign our Acceptable Use Agreements (appendices 3-5).

5.1.1. Use of Email

The school provides each member of staff and pupil with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Staff should also be mindful of using the autofill function in the addressee bar to ensure addressees are not chosen in error.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the Trust Business Manager immediately and follow our data breach procedure.

Spam or junk mail will be blocked and reported to the email provider.

If staff or pupils receive offensive communication, they must inform the Trust Network Manager and this will be recorded in our safeguarding files/records.

Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, pupils and parents.

The school provides each pupil with an email address via the Purple Mash platform that can only be used via this programme and all can be viewed and accessed by the class teacher.

5.1.2. Use of Personal Devices and Mobile Phones

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: Safeguarding, Child Protection and Safer Recruitment, Data Protection and Acceptable Use.

Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place during lesson time.
- Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
- Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

Staff must not give their personal phone numbers to parents or students.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

School phones must not be used for personal matters.

In some circumstances, it may be appropriate for staff to use personal mobile phones for work. Such circumstances may include, but aren't limited to:

- Emergency evacuations;
- Supervising off-site trips;
- Supervising residential visits.

In these circumstances, staff will:

- Use their mobile phones in an appropriate and professional manner, in line with our staff code of conduct;
- Conceal their number if using their phones to contact parents;
- In some circumstances staff will use their phones or iPads to take photographs or recordings of students or their work. In these cases staff must ensure that they have checked the student records to ensure a student's photograph can be used before publishing the photograph. Once the photograph has been used in work, posted on social media or stored on the school system the image must be deleted from their device.

If a member of staff breaches our policy, action will be taken in line with our Code of Conduct/Disciplinary policy.

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

5.2. Personal Use of IT

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Associate Headteacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during directed time;
- Does not constitute 'unacceptable use', as defined in section 4;
- Takes place when no pupils are present;
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes.

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1. Personal Social Media Accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

The school has guidelines for staff on appropriate security settings for social media accounts (see appendix 1).

5.3. Remote Access

We allow staff to access some of the school's ICT facilities and materials remotely.

Systems that can be accessed remotely include:

- **Sims via the SCOMIS** remote connection application. Accessed via secure remote desktop session to SCOMIS server infrastructure, logon via individual user logon and password not linked/used to access on any other systems. Complex passwords required, passwords expire every 42 days. Session screen timeout set to 10 minutes. All settings controlled by SCOMIS GDPR compliant policy. Administration by school IT Support Team, access granted to all teaching and support staff who require SIMS access, permissions within SIMS granted by Data Manager.
- **O365 Suite** – Access via Microsoft O365 cloud, logon via individual user logon and password linked to Windows logon. Administered by IT Support Team. Complex passwords required, expiry every 60 days.
- **Firefly** – Access via Firefly Cloud portal, username logon linked to O365 logon, access controlled by IT support team.
- **CPOMS** – Access via CPOMS Cloud portal, administered by school safeguarding lead. Unique logons not linked to other school logons, two-step authentication required (for high level access).

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 Trust's Network Manager may require, from time to time, against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our Data Protection policy.

5.4. School Social Media Accounts

The school has official Facebook, Twitter and Instagram pages, managed by the IT Support Team. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

Social Media accounts set up to represent the school will follow these guidelines:

The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.

Official social media use will be conducted in line with existing policies, including: Anti-bullying, Data Protection and Safeguarding, Child Protection and Safer Recruitment.

All communication on official social media platforms will be clear, transparent and open to scrutiny.

Parents/carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.

We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff must ensure the school has consent to use, post or publish a photograph or video image of a pupil (this information in held on SIMS and by the Admin team).

If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:

- Always be professional and aware they are an ambassador for the setting;
- Disclose their official role but make it clear that they do not necessarily speak on behalf of the setting;
- Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared;
- Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws;
- Ensure that they have appropriate consent before sharing images on the official social media channel;
- Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so;
- Not engage with any direct or private messaging with current, or past, pupils, parents and carers;
- Inform their Line Manager, the DSL (or deputies) and/or the Associate Headteacher of any concerns, such as criticism, inappropriate content or contact from pupils.

5.5. Monitoring of School Network and Use of ICT Facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited;
- Bandwidth usage;
- Email accounts;
- Telephone calls;
- User activity/access logs;
- Any other electronic communications.

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business;
- Investigate compliance with school policies, procedures and standards;
- Ensure effective school and ICT operation;
- Conduct training or quality control exercises;
- Prevent or detect crime;

- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

6. Pupils

6.1. Access to ICT Facilities

- Computers and equipment in the school's ICT suite are available to pupils under the supervision of staff;
- Specialist ICT equipment, such as that used for music must only be used under the supervision of staff;
- Pupils will be provided with an account linked to the school's virtual learning environment, which they can access from any device by using the following URL https://www.purplemash.com.
- Sixth-form students can use the computers in school independently for educational purposes only. (See 9.1).

6.2. Search and Deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search personal property if the schools believes a pupil may have something illegal or dangerous, this includes searching phones, computers or other devices. We work with the Police if we believe the phones, computers or other devices contain illegal material.

The school can, and will delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

6.3. Unacceptable Use of ICT and the Internet outside of School

The school will sanction pupils, in line with the Behaviour and Discipline policy if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright;
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination;
- Breaching the school's policies or procedures;
- Any illegal conduct, or statements which are deemed to be advocating illegal activity;
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate;
- Activity which defames or disparages the school, or risks bringing the school into disrepute;
- Sharing confidential information about the school, other pupils, or other members of the school community;

- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel;
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities;
- Causing intentional damage to ICT facilities or materials;
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation;
- Using inappropriate or offensive language.

7. Parents

7.1. Access to ICT Facilities and Materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the Associate Headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2. Communicating with or about the School online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to sign the agreement in appendix 2 when their child starts school.

8. Data Security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1. Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

All users are expected to log-off or lock their screens/devices if systems are unattended.

The school requires password updates every 60 days.

8.2. Software Updates, Firewalls, and Anti-virus Software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

8.3. Data Protection

All personal data must be processed and stored in line with data protection regulations and the school's Data Protection policy.

8.4. Access to Facilities and Materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the Trust Network Manager.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Trust Network Manager immediately.

Users should always log-out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

9. Internet Access

The school wireless internet connection is secured.

Separate Wi-Fi connections are maintained for:

- School owned equipment, radius authenticated using staff/pupil Windows logon and password;
- Non-school owned equipment being used by staff/pupils isolated connection allowing internet access but no access to internal school servers/systems. Authentication from splash screen by school Windows logon and password;
- Guest access – time limited accounts configured on an individual basis by the IT Support Team. Again access via splash screen using the temporary logon/password allocated. No access to internal systems.

In all cases internet access is appropriately filtered dependent on the user being a staff, pupil or guest using a commercial firewall/web filter that offers full SSL decryption and inspection. Age appropriate categories are applied to pupil year groups. This firewall/filter are managed by the IT Support Team.

9.1. Pupils

Currently only 6th form pupils are allowed Wi-Fi access, this is managed by the IT Support Team and restricted by individual device addresses of pupil, phones, tablet, laptops being added specifically to grant access to the non-school owned equipment Wi-Fi provision. Access is via school pupil Windows logon to the splash screen and is filtered by the standard 6th form pupil access restriction policy.

9.2. Parents, Visitors and Governors

Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the Associate Headteacher.

The Associate Headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the 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);
- Governors will be allowed access to the school's Wi-Fi system when using it for official school business.

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10. The use of IT systems for Teaching and Learning

We recognise that the use of Virtual Learning Environments (VLE), interactive applications, videoconferencing and the use of webcams e.g. Zoom and Skype can bring a wide range of learning benefits.

10.1. Management of Videoconferencing in School

All videoconferencing and/or webcam equipment will be switched off when not in use and will not be set to auto-answer.

Parents/carers consent will be obtained prior to pupils taking part in video-conferencing activities.

In school videoconferencing will be supervised appropriately, according to the pupils' age and ability.

Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.

Video conferencing will take place via official and approved communication channels following a robust risk assessment.

10.2. Management of our Virtual Learning Environment

The Trust Network Manager, Leaders and staff will regularly monitor the usage of the Virtual Learning Environment (VLE) - PurpleMash, including message/communication tools and publishing facilities.

Only current members of staff and pupils will have access to the VLE.

When staff and/or pupils leave the setting, their account will be disabled or transferred to their new establishment.

Pupils and staff will be advised about acceptable conduct and use when using the VLE.

All users will be mindful of copyright and will only upload appropriate content onto the VLE.

Any concerns about content on the VLE will be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive;
- If the user does not comply, the material will be removed by the Trust Network Manager;
- Access to the VLE for the user may be suspended;
- The user will need to discuss the issues with a member of leadership before reinstatement;
- A pupil's parents/carers may be informed.

If the content is illegal, we will respond in line with existing child protection procedures.

There may be times when pupils may require editorial approval from a member of staff to access a page e.g. House Captain access to House pages. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

10.3. Management of Teaching and Learning Applications (Apps)

The school uses a number of online learning applications to enhance learning, e.g. Accelerated Reader.

All pupils are advised regarding safety measures, such as using strong passwords and logging out of systems;

Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

10.4. Management of communication with pupils through the VLE, providing recorded lessons and online lessons using livestreaming, videoconferencing and online tools e.g. Zoom, Teams, Skype.

Set up school accounts for any online platforms you use. Teachers must never use personal accounts or personal phone numbers. This also applies to communication via email.

If recording videos or livestreaming lessons, make sure to film in a neutral area where nothing personal or inappropriate can be seen or heard in the background. You should make sure that the recording or lesson can take place uninterrupted.

If communicating with pupils online, make sure the platform you are using is suitable for their age group. Also check the privacy settings to ensure you are not broadcasting publicly. If you are unsure speak to IT support about how you do this.

Get written consent from parents or guardians and pupils for pupils to be involved in online lessons (appendix 6).

Establish ground rules for 'live streaming' lessons – when can pupils speak – how will they notify the group they want to speak.

Live streaming should always involve a whole group or class never a one-to-one.

If you are live streaming keep a brief log of – what, when, who and make a note of anything that went wrong.

Always let your line manager know when a 'live streaming' lesson will be taking place.

Think carefully about how you will ensure those pupils who cannot access the lesson will be given equality of opportunity. No pupil should be penalised because they do not have access to the appropriate technology.

Remind pupils about the Acceptable Use policies they have signed.

Always try to give feedback via the VLE, if this is not viable then always use your school email account and copy in the parent or your line manager.

If you have any concerns about a child contact the DSL, DSO or Headteacher immediately as per the Safeguarding and Child Protection Policy.

11. Monitoring and Review

The Associate Headteacher and the Trust Network Manager will monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every two years.

The Board of Trustees is responsible for approving this policy.

12. Related Policies

This policy should be read alongside the school's policies on:

- Safeguarding, Child Protection and Safer Recruitment;
- Behaviour;
- Staff Discipline;
- Data Protection.

Authorised by	The Board of Trustees
Date	13th May 2020
Date for Review (2 years)	May 2022

Appendix 1: Facebook Cheat Sheet for Staff

Don't accept friend requests from pupils on social media

10 Rules for School Staff on Social Media Accounts

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead;
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional;
3. Check your privacy settings regularly;
4. Be careful about tagging other staff members in images or posts;
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils;
6. Don't use social media sites during school hours;
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there;
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event);
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information;
10. Consider uninstalling the apps from your phone. Most apps recognise Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or pupils).

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list;
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts;
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster;
- **Google your name** to see what information about you is visible to the public;
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this;
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender.

What do to if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile;
- Check your privacy settings again, and consider changing your display name or profile picture;
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and you will have to notify Senior Leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages;
- Notify the Senior Leadership Team or the Associate Headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school;
    - Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in.
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so.

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way;
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred;
- Report the material to Facebook or the relevant social network and ask them to remove it;
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents;
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material;
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the Police.

Appendix 2: Acceptable use of the Internet: Agreement for Parents and Carers - NEW

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Our official Facebook page; • Email/text groups for parents (for school announcements and information); • Our virtual learning platform. 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).	
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 the school or 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.	
Signed:	**Date:**

Appendix 3: Acceptable Use Agreement for Secondary School Students

Acceptable use of the school's ICT facilities and internet: agreement for students	
Name of student:	
When using the school's ICT facilities and accessing the internet in school, I will not: • Use them for a non-educational purpose; • Use them without a teacher being present, or without a teacher's permission; • Use them to break school rules; • Access any inappropriate websites; • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity); • Use chat rooms; • Open any attachments in emails, or follow any links in emails, without first checking with a teacher; • Use any inappropriate language when communicating online, including in emails; • Use inappropriate names for my work or files or access or change anyone else's work/files; • Share my password with others or log in to the school's network using someone else's details; • Be unkind or bully other people; • Damage the IT equipment. I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's ICT systems and internet responsibly. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (student):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 4: Acceptable Use Agreement for Primary School Pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils

Name of pupil:

When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me;
- Use them to break school rules;
- Go on any inappropriate websites;
- Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson);
- Use chat rooms;
- Open any attachments in emails, or click any links in emails, without checking with a teacher first;
- Use mean or rude language when talking to other people online or in emails;
- Use inappropriate names for my work or files or access or change anyone else's work/files;
- Share my password with others or log in using someone else's name or password;
- Be unkind or bully other people;
- Damage the IT equipment.

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Appendix 5: Acceptable Use Agreement for Staff, Governors, Volunteers and Visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT facilities and accessing the internet in school, or outside 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 Trust's data protection policy.

I will let the Designated Safeguarding Lead (DSL) 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 let the Designated Safeguarding Lead (DSL) and the Trust Network Manager know if a pupil's on line behaviour is inappropriate or concerning in any way.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 6: Pupil User and Parental Agreement for Online Lessons

Pupil user and parental agreement for online lessons	
Name of pupil:	
In the event of your child having to be at home for a period of isolation due to a bubble closure or a full school lockdown. We will be providing some online face-to face sessions to further enhance our pupil's learning. We must receive parental permission before a pupil is able to take part in face-to-face interactions. Alongside the Acceptable Use Agreement already signed by your child, the additional guidelines below outline further expectations. We expect all pupils to adhere to these guidelines in order to engage safely in the face-to-face sessions and ask you to read and discuss these guidelines with your child before signing the agreement below. If you have any concerns or queries contact the Associate Headteacher.	
Guidelines When taking part in livestreaming lessons remember that this is an extension of the classroom and you should conduct yourself as you would in a classroom. This includes: Video conferencing from an environment that is quiet, safe and free from distractions; Be on time for your interactive session; Be dressed appropriately for learning (no pyjamas, no swimwear); Remain attentive during sessions; Interact patiently and respectfully with your teachers and peers; Provide feedback to teachers about your experiences and any relevant suggestions; You **MUST NOT** record or take photos of online interactions; Make sure you end the session as soon as the teacher indicates to do so. I understand that these rules are designed to help keep me safe and that if they are not followed, school sanctions will be applied and my parent may be contacted.	
Signed (pupil):	**Date:**
Signed (parent/carer):	**Date:**