Stogursey C of E Primary
and Pre-School

QUANTOCK
EDUCATION TRUST

ICT AND INTERNET ACCEPTABLE USE POLICY

Approved by: G Tucker		**Date:** 1.9.20
Last reviewed on:	1.9.20	
Next review due by:	1.9.21	

Contents

Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, 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.

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 2018

Searching, screening and confiscation: advice for schools

Roles and Responsibilities

Governors

Governors are responsible for the approval of the ICT and Internet acceptable use policy, ensuring that it is implemented and reviewing its effectiveness. Governors will require information on the following regular activities:

- Monitoring of online safety incident logs.
- Reporting to relevant governor committees.
- Keeping up to date with school online safety matters.

Head of School

The Head of School is responsible for ensuring the overall safety, including online safety, of members of the school community. The Designated Safeguarding Lead (DSL) holds a responsibility for online safety as part of their role (as noted in the 2018 Keeping Children Safe in Education statutory guidance). On a practical day to day basis, others may have particular duties relating to Online Safety, e.g. ICT/Computing Subject Leader, Network Manager/Technician. However, the Head of School will ensure the following:

- Staff with online safety responsibilities receive suitable and regular training enabling them to carry out their online safety roles and to train other colleagues as necessary.
- The Senior Leadership Team (SLT) receives regular monitoring reports.
- There is a clear procedure to be followed in the event of a serious online safety allegation being made against a member of staff.
- Take a leading role in establishing and reviewing the school's Online safety and ICT and internet acceptale use policies and associated documents.
- Provide training and advice for staff and ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provide materials and advice for integrating online safety within schemes of work and check that online safety is taught on a regular basis in conjunction with the Computing Lead.
- Liaise with the school's IT technical staff.
- Ensure that online safety incidents are reported and logged and used to inform future online safety developments.
- Report to the governors and meet with them as required.

IT Technician/Support Provider

The IT Technician/Support Provider will be responsible for ensuring that all reasonable measures have been taken to protect the school's network. This will involve ensuring the following:

- The IT infrastructure is secure and protected from misuse or malicious attack.
- The school meets the online safety technical requirements outlined in any relevant online guidance.
- Users may only access the school's network through a properly enforced password protection policy.
- The school's filtering policy is applied and updated as appropriate.
- Any inappropriate use of the school's computer systems should be reported to the appropriate senior person.
- Provide secure external access to the school network as appropriate.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They are familiar with current online safety matters and the school's Online Safety Policy and practices.
- They have read and understood the school's Staff ICT and Internet Acceptable Use Policy and signed to indicate agreement.
- They report any suspected misuse or problem to the Head of School for investigation and action.
- Electronic communications with pupils should be on a professional level and only carried out using approved school IT systems.
- Online safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the school's Online Safety and Acceptable Use Policies.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations in relation to their age.
- They monitor IT activity in lessons, extra-curricular and extended school activities.
- They are aware of online safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement school policies with regard to these devices.
- They know and follow the procedure for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead (DSL)/Child Protection Officer(CPO)

The DSL/CPO holds the responsibility for online safety as part of their role (as noted in the 2018 Keeping Children Safe in Education statutory guidance). They should be trained in online safety issues and be aware of child protection matters that may arise from any of the following:

- Sharing or loss of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyberbullying

Data Protection Officer (DPO)

The DPO has a related role which is detailed in Data Protection policies and related documentation.

Reviewing, Reporting and Sanctions

Review

- This policy will be reviewed and updated every two years, or more often if necessary.
- The school will audit provision to establish if the Online Safety Policy is adequate and that its implementation is effective.

Acceptable Use Agreements

- All users of school IT equipment will sign the appropriate Acceptable Use Agreement. This includes all staff and KS2 pupils.
- Parents may be asked to sign on behalf of their children or to show agreement with and support for the school's policy.

Reporting and logging

- The school will produce clear guidelines as to what should be done if inappropriate content is found when accessing the internet.
- Any such occurrence will be logged for review and any necessary actions that arise.
- All pupils and teachers should be aware of these guidelines.

Complaints regarding internet use

- Any complaints relating to internet misuse should be made in accordance with the school's existing complaints procedure.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Sanctions

- Failure to comply with the requirements of this policy will be dealt in line with the school's existing policy on behaviour.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 or other related legislation. This would constitute a disciplinary matter in the case of staff.

Communications & Communication Technologies

Mobile phones and personal handheld devices

- Pupils will not be allowed to bring mobile phones to school.
- Pupils will not be allowed to bring in games devices, particularly those which allow ad hoc networks to be established.
- Teacher/parent contact should normally be by the main school telephone or via the Admin e-mail address and not via a mobile device except where off-site activities dictate the use of a mobile phone.
- Parent helpers in school and staff must ensure that they do not send personal messages, either audio or text, during contact time with pupils. If an exceptional emergency arises, they should arrange temporary cover whilst they make a call.
- Staff and pupils may send educational messages during lesson times if these are part of the curriculum.
- Staff, helper and visitor mobile devices should be switched off or to silent mode during the times that children are present.
- No device in any school building should contain any content that is inappropriate or illegal.

Personal Use

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 Head of School may withdraw permission for its' use at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time.
- Does not constitute 'unacceptable use,' as defined in 'Internet Usage' page 7.
- 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 as defined in 'Security' page 9. Where breaches of this policy are found, disciplinary action may be taken. Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's mobile phone and this policy.

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.

School social media accounts

The school has an official Facebook page, managed by the Head of School. Staff members who have not been authorised to manage or post to the account, must not access, or attempt to access the account.

E-mail and messaging

- Pupils and staff will be informed that the use of school e-mail or messaging accounts may be monitored.
- Pupils should report any receipt of an offensive e-mail or message on school IT systems.
- Pupils should not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone via an e-mail or message.
- Information of a sensitive nature should not be sent by unencrypted e-mail.

Social networking

For the purpose of this policy, social networking is considered to be any digital media or medium that facilitates interaction.

- Staff use of social networking should be compatible with their professional role and show the highest standards of integrity.
- Pupil use of social networking should conform to age restrictions.

Internet Usage

The school will take all reasonable precautions to ensure that pupils' access only appropriate material. Whilst it is not possible to guarantee that unsuitable material will never appear on a school computer, the school will take appropriate measures to prevent a reoccurrence, including contacting the service provider.

All users using the internet, and associated communication technologies, will be made aware of the school's online safety guidelines and will receive guidance in responsible and safe use on a regular basis.

The school will sanction pupils/staff, in line with the behaviour/discipline policy, if they engage in any of the following at any time (even if they are not on school premises):

- Breaching the school's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, other pupils/staff, 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.
- Download, upload, display or access knowingly, sites that contain pornography or other unsuitable material that might be deemed illegal, obscene or offensive.
- Attempting to disable, bypass or reconfigure any filtering, virus protection or similar.
- Using ICT or the internet to breach intellectual property or copyright.
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination.
- Using inappropriate or offensive language.
- Causing a data breach by accessing, modifying, or sharing (including personal data) to which a user is not supposed to have access or without authorisation.

Digital and video images

Parental permission

- The school will ensure that, where appropriate, consent is obtained for the taking and use of digital and video images of pupils. Such use could include the school website or social media; display material in and around the school or off site; the school prospectus or other printed promotional material; local/national press.
- Pupils will not be identified by name in any title or commentary accompanying digital or video images that is in the public domain, unless specific parental consent has been obtained.
- Where parental permission has not been obtained, or it is known that a pupil should not be photographed or filmed, every reasonable effort should be made to ensure that a pupil's image is not recorded.

Storage and deletion

- Images should be uploaded to a secure location that is the control of the school. Where memory cards, USB drives, CDs or cloud storage are used during the process of capture or transfer, users should ensure that these are deleted and cleared from any temporary storage or recycle bins.
- Images should be deleted in line with the school's procedures on data retention and disposal.

Recording of images

- School digital devices should always be used to record images of pupils.
- All pupils appearing in images should be appropriately dressed.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- All digital devices capable of taking photographs and recording sound or video, whether belonging to the school or personal, may be subject to scrutiny if required.
- Where volunteers are supporting school staff, they should abide by the same rules as school staff.

Parents taking photographs or video

Where the school chooses to allow the recording of images at 'public' events, the following should apply:

- Images may only be recorded for personal use and can only be shared with family and friends. They must not be shared on social networking sites or other websites that are accessible by the general public.

Events/Activities involving multiple schools

- When taking part in events organised by other schools or organisations, e.g. sports or music events, the schools involved will consider what image guidelines should apply.
- For larger events it is reasonable to expect that specific image guidelines should be in place. Where relevant these should include reference to press images.
- Consideration should be given as to how those attending the event will be informed of the image guidelines that apply, e.g. a letter before the event, announcement at the event, or information in any printed programme.
- Although the school will make reasonable efforts to safeguard the digital images of pupils, parents should be made aware that at some types of event it is not always realistic to strictly enforce image guidelines. The school cannot therefore be held accountable for the use of images taken by parents or members of the public at events.

Infrastructure and Security

Security

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that procedures outlined within this policy are implemented by those responsible.

- School IT technical staff may monitor and record the activity of users on the school IT systems and users will be made aware of this.
- Servers, and communications cabinets should be securely located and physical access restricted.
- Wireless systems should be appropriately secured.
- All users will have clearly defined access rights to school IT systems.
- Access to the school IT systems will cease when a pupil leaves or, in the case of a member of staff, ceases to be employed by the school.
- Appropriate procedures should be in place for secure storage and access to 'Administrator' passwords.

Passwords

All staff are provided with an individual password. Pupils will have an individual password for accessing the network, though a group password may be acceptable for young children.

The IT manager should advise staff on the choice and use of passwords. The following areas may also be appropriate:

- 'Strong' passwords should be used.
- Users are responsible for security of their passwords and accounts, and for setting permissions for accounts and files they control.
- No individual should tell another individual their password.
- No individual should log on using another individual's password, unless they are a member of staff logging on as a pupil for sound educational or technical reasons.
- Once a computer has been used, users must remember to log off.
- Users leaving a computer temporarily should lock the screen (Windows key + L on a PC/Laptop).

Filtering

The school maintains and supports the managed filtering service provided by the support provider. Changes to network filtering should be approved by the appropriate person(s).

- Any filtering issues should be reported immediately to IT Technician or the support provider.

Software updates/Firewall Virus protection

- All computer systems, including staff laptops/devices, should be protected by an antivirus product which is administered centrally and automatically updated.

Staff laptops/devices and flash drives

Where staff laptops/devices and flash drives are to be taken out of school, it is possible that they may contain sensitive data, therefore the schools should ensure that all such devices and removable media are encrypted.

The following security measures should also be taken with staff laptop/mobile devices:

- Laptops/devices must be out of view and preferably locked away overnight whether at school or home.

- Laptops/devices should not be used for purposes beyond that associated with the work of the school, e.g. by the family of a member of staff.
- Where others are to use the laptop, they should log on as a separate user without administrator privileges.

Data protection

All personal data must be processed and stored inline with data protection regulations and the school's data protection policy.

See Data Protection Policy for specific guidance in relation to the security of personal data.

Electronic devices - 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 pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

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.

Online Safety Education

Learning and teaching for pupils

- Computers and equipment in the school are available to pupils only 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 their personal login details.
- Pupils should be encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside school.
- Pupils should be helped to understand the need for an Acceptable Use Policy and, depending on age, asked to sign to indicate agreement.
- Pupils should be taught to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Key online safety messages will be included within the curriculum and reinforced as part of a planned programme of assemblies and other appropriate opportunities.
- Rules for the use of computers/devices should be displayed in all rooms and displayed next to fixed site computers.

Staff training

- Staff will be kept up to date through regular online safety training.
- Staff should always act as good role models in their use of IT, the internet and mobile devices.

Parental support

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 FOSS) may be granted an appropriate level of access, or be permitted to use the school's facilities at the Head of School's discretion.

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

The support of, and partnership with, parents should be encouraged. This is likely to include the following:

- Awareness of the school's policies regarding online safety and internet use; and where appropriate being asked to sign to indicate agreement. (Appendix 4)
- Practical demonstrations and training
- Advice and guidance on areas such as:
    - filtering systems
    - educational and leisure activities
    - suggestions for safe internet use at home

Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the Head of School.

The Head of School 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 FOSS)

Visitors including Governors who need to access the school's wifi 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)

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

Monitoring and review

The Head of School and IT Manager 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 2 years.

The governing board is responsible for approving this policy.

Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection

Appendix 1 – Course of action if inappropriate content is found

- If inappropriate web content is found (i.e. that is pornographic, violent, sexist, racist or horrific) the user should:
    - Turn off the monitor or minimise the window.
    - Report the incident to the teacher or responsible adult.
- The teacher/responsible adult should:
    - Ensure the well-being of the pupil.
    - Note the details of the incident, especially the web page address that was unsuitable (without re-showing the page to the pupils).
    - Report the details of the incident to the Head of School.
- The Designated Safeguarding Lead, Head of School or another appropriate person will then:
    - Log the incident and take any appropriate action.
    - Where necessary report the incident to the Internet Support Provider so that additional actions can be taken.

Appendix 2 – Social networking guidelines

Staff conduct

- *Staff will always conduct themselves with the highest standards of professional integrity and be aware that how they as individuals are perceived in the virtual world may reflect on how the school is perceived.*
- *Staff should give careful consideration when posting personal information as to how this might be viewed by pupils and parents, even when the postings are within a 'private' online space.*

Access to social networking sites

- Social networking sites should never be accessed during timetabled lessons and other contact with pupils and not normally during school working hours.
- Staff may not use school equipment to access social networking sites.
- *If the school chooses to make 'official' use of social networking sites this should only be by authorised individuals.*

Posting of images and/or video clips

- Photographic images and/or movie clips of children at the school or past pupils, up to the age of 18, should never be posted unless specific consent has been obtained.
- Photographic images and/or movie clips of school staff should not be posted unless specific consent has been obtained.

Privacy

- *Staff should recognise that their existing lists of friends/contacts/followers may include people who are part of both their private and professional lives.*
- *Staff should never be online 'friends' with children at the school or past pupils up to the age of 18.*
- *Staff should not create new links with parents at the school, unless there is a professional reason for doing so. In such instances there should be a clear understanding of the purpose of the link and what 'information' the parent will have access to.*
- *Profile settings should be regularly checked, and updated as necessary, to ensure that posted comments and images are not publicly accessible.*
- *Any changes to social networking sites and privacy settings should be clearly understood.*

Stogursey Church of England Primary School and Pre School

"Grow in the Grace and Knowledge"
2 Peter 3:18

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 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.

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

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

Stogursey Church of England Primary School and Pre School

"Grow in the Grace and Knowledge"
2 Peter 3:18

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/School Website 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 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:

Stogursey Church of England Primary School and Pre School

“Grow in the Grace and Knowledge”
2 Peter 3:18

Acceptable use of the school’s ICT facilities and internet: agreement for pupils and parents/carers

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.
- Share my password with others or log in using someone else’s name or password.
- Bully other people.

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 I am responsible for my actions, both in and out of school.

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:**

Stogursey C of E Primary and Pre-School

QUANTOCK EDUCATION TRUST

Facebook Cheat Sheet for Staff

Don't accept friend requests from pupils on social media

10 rules for school staff on Facebook

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 Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi 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**. 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**.

- 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 that if they persist, you'll 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 Head of School 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.