# ICT and Internet Acceptable User Policy

John Hampden and Tetsworth Schools' Federation

| | |
|---|---|
| **Policy Name** | **ICT and Internet Acceptable User Policy** |
| **Adopted** | By: Full Governing Board<br>Date: September 2025 |
| **Signed on behalf of the board** | Natalie Henderson |
| **Headteacher** | Paul Hankey |
| **Review period** | Annually |
| **Date of next review** | January 2028 |

## Contents

# 1. 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 staff code of conduct/ disciplinary process.

# 2. Relevant legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also considers the National Curriculum computing programs of study.

# 3. Definitions

**"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, 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 includes:

- 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
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, 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, deleting or disposing of ICT equipment, systems, programs 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 Headteacher /Head of Teaching and Learning or any other relevant members of staff will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of either 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 Headteacher / Head of Teaching and Learning's discretion. The Headteacher/Head of Teaching and Learning will need to be approached directly and a clear and detailed explanation as to why an 'unacceptable use' would be needed. This would also need to be written in a formal email so we have recorded evidence.

### 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 Code of Conduct/Disciplinary Process.

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

## 5.1 Access to school ICT facilities and materials

The school's Computing Co-ordinator, Computing Support (123ICT) and/ Headteacher or Head of Teaching and Learning 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 their Computing Co-ordinator and /Headteacher or Head of Teaching and Learning

### 5.1.1 Use of phones and email

The school provides each member of staff 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. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

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 their Headteacher/Head of Teaching and Learning immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must, where possible, use phones provided by the school to conduct all work-related business (see Mobile Phone Policy)

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.

## 5.2 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 Headteacher /Head of Teaching 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 contact time/teaching hours/non-break 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 are also permitted to use their personal devices (such as mobile phones, smart watches or tablets) in line with the school's mobile phone 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.

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.

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

## 5.3 Remote access

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

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 guarding against the importing of 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 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

Prevent or detect crime

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

# 6. Pupils

## 6.1 Access to ICT facilities

Computers and equipment in the school are available to pupils only under the supervision of staff.

Computers are timetabled accordingly so classes have access to both laptops and iPads regularly.

Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff"

All stand-alone computing equipment is password protected and is inaccessible to the children.

## 6.2 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with our behaviour policy/ICT policies, 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 Headteacher /Head of Teaching and Learning'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 look at the Parents Code of Conduct (see Appendix 1) and adhere to these rules.

# 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.

Children from Years 3-6 have their own passwords to access the schools network. These are given to the children's class teacher and children only have access to them during IT lessons. The children are made aware that this must be kept secure.

## 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.

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 their Headteacher/ Head of Teaching and Learning 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 and is monitored by 123ICT.

If inappropriate material (that filtering has missed) comes through then it is the responsibility of the class teacher to report this to either the Computing Co-ordinator or 123ICT.

## 9.1 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 Headteacher / Head of Teaching and Learning

The Headteacher / Head of Teaching and Learning 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 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.

## 10. Monitoring and review

The Computing Co-ordinator and Headteacher / Head of Teaching and Learning 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 2 years.

## 11. Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff Code of Conduct
- Data protection

# Appendix 1

## Internet Code of Conduct for Staff

ICT in its many forms – internet, email, mobile devices etc – are now part of our daily lives. It is our duty to ensure that they are used safely and responsibly. All staff in the John Hampden Primary and Tetsworth Primary Schools' Federation are aware of the following responsibilities:

**You should**:

1. All Staff understand that ICT includes a wide range of systems, including mobile phones, digital cameras, smart watches, laptops and tablets.
2. All staff will ensure their class is aware of Internet safety issues, including cyber-bullying, and how to deal with these responsibly.
3. All staff will ensure that all children have read and returned their Internet Code of Conduct form. The staff will need to check at the beginning of each academic year to see which children have not read/signed this form as children will not be allowed to use the Internet in school.
4. All staff will ensure that data is kept secure and is used appropriately as authorised by the Head Teacher/Head of Teaching and Learning.
5. All staff should treat sensitive, personal information about pupils with respect and confidentiality and never disclose it on the Internet.
6. Neither teacher nor children's passwords should be divulged or displayed. Passwords should be given to the individual Key Stage 2 child only.
7. All staff will ensure that all children using the Internet are supervised at all times.
8. All staff will ensure that sites pre-selected for children's use are appropriate to the age and maturity of the pupils.
9. All staff should be aware that others, including children, can see your actions on the Internet.
10. All staff should only access sites that are appropriate for use in school. This also applies outside of lesson time.
11. All staff will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
12. All staff understand that they are responsible for all activity carried out under their username.
13. All staff should respect copyright and trademarks. You cannot use the words and pictures that you see on some Internet sites without giving credit to the person that owns the site.
14. All staff should think carefully about the trustworthiness of a website before downloading files and programs, opening e-mail attachments or completing subscription forms.

15. All staff should ensure that all content to be used on the school website is accurate and appropriate.

16. Staff will not install any software or amend/alter software on any school owned device without the school's technician's permission.

17. All staff understand that their use of the internet may be monitored and if anything untoward is uncovered, could be logged and used in line with any disciplinary procedures. This includes all school owned devices. If an E-safety incident should occur, staff will report it to the Head teacher as soon as possible.

18. All staff will only use the school's email system for school correspondence not their own personal use. Likewise, they should not use their personal emails for school use.

19. Personal mobile phones, smart watches or digital cameras must NEVER be used for taking any photographs related to school business.

20. Images will only be taken, stored and used for purposes within school unless there is parental permission for alternative use. At the start of each year, our parents are asked to opt out if they don't agree to their children's images being used. If a parent chooses to opt out, we ensure that their child's photograph is not used.

21. All staff will report any incidents of concern regarding staff use of technology and/or children's safety to the Head or the Designated Professional in line with our school's Safeguarding Policy.

22. All staff understand that it is a disciplinary offence to use the school ICT equipment for the use of gambling, advertising or soliciting for personal gain, to post or forward chain letters and other unacceptable use.

Signed: _____

Print name: _____

Date: _____

# Appendix 2
# Children's Internet Code of Conduct

Dear Parents/Guardian,

As part of our curriculum we encourage pupils to make use of educational resources available on the Internet. Access to the Internet enables pupils to conduct research and obtain high quality educational resources from libraries, museums, galleries and other information sources from around the world.

To guard against accidental access to materials, which are inappropriate in school, our school access' the Internet by means of a web filter service by RM. However, it is not possible to provide 100% assurance that pupils might not accidentally come across material, which would be inappropriate.

Therefore, before they access the Internet we would like all pupils to discuss the attached Internet Code of Conduct with their parents/guardians and then return the attached form to their teacher. This is for the duration of their academic life at the John Hampden Primary and Tetsworth Primary Schools' Federation.

We believe that the educational benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, far outweigh the potential disadvantages.

During lesson time teachers will guide pupils toward specific materials and educational resources. Where pupils are given permission to access the Internet outside lessons they must agree to access only those sites that are appropriate for use in school.

Yours sincerely

Mrs Schleising and Mr Hankey (JHS) Mrs S Spencer (TPS)

# CODE OF CONDUCT FOR THE USE OF COMPUTING AT SCHOOL

This code of conduct applies at all times when using school equipment. It is compulsory that you complete this form, for your child to be allowed to use the school ICT system, including use of the internet. Please ensure that you have read and understood the terms of our Computing Code of Conduct. We have also attached a child friendly code of conduct for your child to keep, which highlights how to stay safe. The staff are working incredibly hard to ensure that the children are aware of online-safety and would like your support by reinforcing this at home when you are using computer based technology.

## THE CODE

**Your child should:**

- Only access websites that are appropriate for use in the school (including outside of lesson times)
- Be aware that your actions on the Internet can be seen by others.
- Be careful of what you say to others and how you say it. *Never give your name, home address, telephone numbers or any personal information about yourself or others to any strangers you write to or talk with on the Internet.*
- Respect copyrights (i.e. do not use text/images found on the internet and credit them as being your own work)
- Report anything that they feel is inappropriate or offensive to their teacher

**Your child should not:**

- Give their usernames and passwords to anyone
- Send, access or display offensive messages or pictures
- Send or collaborate in hurtful messages or e-mails. Cyber bullying will not be accepted
- Use or send bad language
- Intentionally waste resources

**Please note:**
User areas on the school network will be closely monitored and staff may review your child's files and communications to maintain system integrity. Failure to follow this code of conduct will result in loss of access and further disciplinary action may be taken if appropriate. If applicable, external agencies may be involved: certain activities may constitute a criminal offence.

---

Pupil's Name_____ Class_____

Please sign in the space below to acknowledge that you and your child have read and discussed the Computing Code of Conduct. If pupils fail to follow the Code of Conduct, parents will be informed and access will be withdrawn.

Parent/guardian signature: _____

*(Please hand this form back to your teacher a.s.a.p. Failure to do so will result in your child being denied access to the Internet within school)*

John Hampden Primary School | Tetsworth Primary School

John Hampden and Tetsworth Schools' Federation

# *John Hampden Primary School*
# *Computing Code of Conduct*
# *Be Responsible Stay Safe on computers*

These rules for sensible Internet and ICT use will ensure our safety. Please make sure you understand them and keep them

Use of computers is for educational purposes.

1. Only use the Internet when there is a teacher or other adult present to supervise, or when you have permission.
2. Only use your own login and password.
3. Never give out your address, phone number or arrange to meet someone.
4. All e-mails should be polite, appropriate and sensible.
5. If you receive a rude or offensive message you must report it to a member of staff immediately.
6. If you see anything offensive or if you feel uncomfortable about anything report it.
7. Be aware that the school may check your computer files and monitor the Internet sites you visit.
8. Make sure that a web source is reliable and information you are going to use is accurate.
9. John Hampden Primary School has a zero tolerance policy to any type of Cyberbullying. Anyone found to be doing this will be warned and possibly denied access to Internet resources.

I understand that if I break any of these rules I will be moved off the computer and my parents will be informed.

**Be Sensible and Be Safe!**

**Device/Mobile Phone/Smart Watch Code of Conduct**

**Mobile Phones**

Within the John Hampden and Tetsworth School Federation, children in Year 5 and Year 6 will be permitted to bring a mobile phone to school, where parents/carers are in agreement, and where possession of a mobile phone would be of significant and demonstrable benefit to the child.

Children in years Reception to Year 4 are not permitted to bring a mobile phone to school.

Mobile phones must be switched off and handed to the class teacher on entry into school and will not be allowed to be used during the school day. The school will accept no responsibility for any subsequent damage or loss.

**Smart Watches**

Within the John Hampden and Tetsworth School Federation, children are not permitted to wear smartwatches with camera facilities and independent access to the internet. Analogue watches or a basic activity tracking watches (such as Fitbits) are allowed, if a staff member is in any doubt as to whether the watch is against our policy we reserve the right to confiscate it until we have discussed the matter with the parents/carer of the child.

**Any child found to be inappropriately using a mobile phone or smart watch will have their device confiscated and kept by the school until appropriate arrangements can be made for the collection of device by a parent/carer. The child will not be able to bring in a mobile device into school from this point and will be dealt with in accordance with the school Behaviour Policy.**

**Parents/Carers who need to contact their child in the case of an emergency should always do so by contacting the school office.**

---

**Mobile Phone Parental Consent**

I give permission for my child …….. to bring their mobile phone to school. I have read the policy and understand the implications.

Signed:

Date:

Please return to the school office. Thank you

## FILM AND VIDEO

Occasionally we use U/PG rated films and educational videos as tools for teaching and learning (in preparation for a production or to compare and contrast film and text for example). These will always be watched under supervision.

I am happy for my child to watch U/PG rated films and educational videos as part of their learning.

Signed:_____(Parent/Guardian)

If at any time you would like to withdraw your permission during your child's time at either John Hampden Primary School and/or Tetsworth Primary School, please inform the office.

## Evidence Me

At John Hampden Primary School and Tetsworth Primary School, we use an iPad app called Evidence Me to collect and collate observations of the children which help us to assess their learning and progress throughout their time in the Early Years Foundation Stage.

Often, observations include learning experiences that involve more than one child and therefore photographs and first names of other children may appear in your child's learning journal. It also means that your child's first name and photo might appear in another child's journal.

At the end of their time in Nursery or Reception, your child will be able to bring their 2Simple journal home. With new guidelines, we now have to ask parents if they are happy for photographs of their child to appear in other children's journals. These journals are for personal use only and we ask that they are not shared on social media in any way.

We would appreciate a signature to confirm that you are happy for your child's first name and photograph to appear in another child's journal if they are involved in a joint learning experience.

We thank you for your support and look forward to sharing your child's learning with you,

The EYFS Team.

- I understand that when I receive the hard copy of my child's Evidence Me profile, it is for personal use and should not be shared on social media.
- I give permission for joint observations of my child to be included in the Evidence Me observations of other children.

Parent/guardian signature:_____

# Appendix 3

| Acceptable use of the internet: agreement for parents and carers | |
|---|---|
| **Name of parent/carer:**<br><br>**Name of child:** | |
| Online channels are an important way for parents/carers to communicate with, or about, our school.<br>The school uses the following channels:<br>• Our official Facebook page<br>• Email/text groups for parents (for school announcements and information)<br>• Our virtual learning platform<br>Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, 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:<br>• Be respectful towards members of staff, and the school, at all times<br>• Be respectful of other parents/carers and children<br>• 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<br><br>I will not:<br>• 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<br>• 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<br>• 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 4:
# Facebook cheat sheet for staff

**Don't accept friend requests from pupils on social media**

10 rules for school staff on Facebook

1. You might want to consider changing your display name. You could use your first and middle name, use a maiden name, or put your surname backwards instead
2. You might like to 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. Ask their permission first.
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** – 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 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 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