Norton Community Primary School

Acceptable Use Policy

Information and Communication Technology

September 2018

This policy replaces and supersedes the following:

Acceptable Use Policy (2015 – 2017)
Staff Email and Internet Policy (2015 - 2017)
Social Media Policy 2016

Vision Statement

Nothing is beyond our reach!

Care and challenge engage and motivate us!

Praise reassures and supports us!

Successes are celebrated and built on!

Contents

Introduction

This document is for parents, governors, staff and children. It specifies the acceptable use of information and communication technology systems, services and equipment (ICT). It covers ICT provided by the school and the use of individual's own ICT when used on school premises or upon school business. It covers use of all forms of online/internet ICT including email and social media.

Monitoring and Protection

In order to keep school systems secure and available for all, and to help protect everyone in our learning community we use a number of systems for both monitoring and protection.

- SMOOTHWALL - managed jointly by the school and by North Yorkshire Schools ICT.
- SOPHOS ANTI-VIRUS

Monitoring

SMOOTHWALL is a combined firewall, content filter and network monitoring tool. The network monitoring facilities in SMOOTHWALL allow internet access to be tracked against your school network login account. For example, websites visited, search keywords used and files uploaded or downloaded. Notably, attempts to access sites flagged within SMOOTHWALL as inappropriate are logged.

Staff are provided with a Microsoft Office 365 account for email, collaboration and data storage. Office 365 is continually enhanced with features that support monitoring and audit of information transmitted through and stored within it.

Specific applications are used by staff to record information about learners and the day-to-day business of the school (e.g. SIMS, OTrack and Tapestry). Monitoring and audit facilities may be provided within these systems. For example, it may be possible to match up data changes, exports or deletions to the user account that was used to do them.

The school may use any of these monitoring features in the course of an appropriately authorised investigation.

Staff should be aware that:

- All web activity (searches, uploads, downloads) can be logged and analysed
- Anything sent through the school email system may be accessed and viewed by senior leaders. Anyone whose account has been accessed in this way will be informed.
- Application audit logs may be analysed

Light touch auditing and monitoring facilities may be used periodically to ensure that systems are only being used for operational reasons that enhance teaching and learning. The specific content of any transactions will only be monitored if there is a suspicion of unacceptable use.

Protection

SMOOTHWALL's firewall provides protection against electronic attacks against our devices and the content filter prevents access to websites and types of content marked as inappropriate. There are different levels of filtering set up for staff and pupils. For example, pupils are blocked from accessing YouTube videos whereas staff logins can do so.

It is important for members of staff to know that they have wider internet access than pupils and to make sure that equipment is locked when left and that pupils are not allowed to use staff level accounts.

Equipment and Software

School Equipment

- Take care of school equipment so that accidental damage is minimised.
- Do not deliberately damage equipment.
- Notify IT Support of any damage to equipment.

Restrictions on the school network will prevent you from installing additional software, for example, by using the Windows Store. You should not attempt to circumvent these restrictions as new software may have wide-ranging permissions that compromise the security of both your machine and the network.

You should only install additional hardware (e.g. printers, scanners, mice, speakers) if you have first checked with IT Support.

Working Away from School

You should take care when using or transporting equipment away from the school site. You will be responsible for taking all due care to ensure that it is kept safe and is not lost or stolen.

You should take great care to ensure that data and information on your machine is not accessed by anyone else. You should use your passwords according to SKULL principles (see Security and Privacy), especially ensuring that devices are locked when you leave them and logged out when you are finished.

Memory sticks are not secure and are easily mislaid. The school provides an Office 365 account including Microsoft OneDrive as a much better alternative and it is to be used instead. If there is no alternative to using a memory stick, then the memory stick must be encrypted.

Using Your Own Equipment (BYOD)

Pupils

Pupils may not bring their own devices to use in school. If carried, mobile phones must be given in to the school office before registration. They will be kept securely and re-issued to pupils at home time.

Staff

The school provides staff with the ICT equipment that they need to do their job. Therefore, it is unlikely that there will be a need to connect your laptop or tablet to the school network.

Connecting your mobile phone to the school network *may* be allowed. However, it must be done with permission and assistance from IT Support. This is to ensure it is both protected by and monitored by our SMOOTHWALL (see Monitoring) and does not itself pose a risk to the network. When using the device connected to the school WiFi, you may not have access to all your services. For example, your email provider may be blocked by Smoothwall.

Whether or not your phone is connected to our network, there are particular restrictions regarding its use in school.

- Phones **must** be in silent mode or switched off during school hours and should not be checked for personal messages while teaching is in progress.
- You **must never** use your phone to take images or video of either children or documents. This is in line with our safeguarding obligations, and protects learners, staff and the reputation of the school. Mobile services often back up photos to cloud storage automatically and this would result in personal data immediately leaving our control.

Security and Privacy

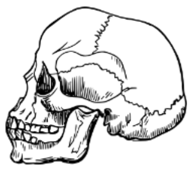
Security

Use of passwords is designed to keep our data safe and to ensure that only you have access to your work. It also helps us track who is using resources and how they are using them. You will be asked to set and manage passwords for access to:

1. The school Windows network, accessible from PCs on school premises
2. Your school Office 365 account @norton-pri.n-yorks.sch.uk
3. Additional ICT services as required (e.g. Purple Mash, OTrack, SIMS, etc.)

Where you are asked to choose and manage your password:

- **S**trong passwords (as appropriate for your age) must be used
- **K**eep it secret (known only to yourself)
- **U**pdate it regularly (there may be prompts to do this)
- **L**ock your account when away from the desk or device
- **L**og out when you have finished.



SKULL

Strong, **k**ept secret, **u**pdated, **l**ocked, **l**og out

If someone else uses your account, and you have told them your password, **you will be held equally responsible for their actions**. If you think that someone else has accessed or tried to access any of your accounts, please tell the IT Support immediately.

At school, you have access to shared drives on the network. These are provided to help us work together and share information. Take extra care when working in shared spaces to avoid accidentally moving or deleting others' work. Do not abuse these facilities to try to gain access to areas that you are restricted from. If you are able to see files and content that you don't think you should, tell IT Support.

If you have access to confidential or personal information as part of your work, this must be kept only in the designated secure areas and applications. You must not disclose any personal information to anyone who does not have a right to see it.

Privacy

The school is the data controller for a range of personal data as detailed in **Norton C P School's GDPR Privacy Notice** (2018). This means the school determines the purposes for which, and the manner in which, any personal data relating to pupils, their families and members of staff is to be processed.

Documents

Documents containing personal data should be stored only in folders on the shared network drives allocated for the purpose or in your secure Office 365 One Drive storage.

Printing

When documents are printed, the information they contain immediately leaves the realm of electronic control and audit. Anyone who comes into possession of the document can read it, copy it and distribute it both physically and electronically through services beyond our control.

We must take all reasonable precautions to protect the personal data that we control, and this includes being careful with printed material. When you are required to print a document that contains personal data:

- Decide if it is really necessary to print the document. It may be just as easy to refer to it on screen or there may be a more secure way to send the document to an authorised third party.
- Ensure that you select the 'Hold print' feature and that your Windows username is used to refer to the held print job.
- Go to the printer as soon as possible to release and print the job. Do not ask another member of staff to do this for you.
- Keep the document for as short a time as necessary. Keep it secure and in locked storage when it is out of your immediate possession. Shred it as soon as you no longer need it.

If you find a printed document that has been left unattended and you become aware that it contains personal data:

- Stop reading the document beyond the point you realise that it contains personal data.
- Shred it immediately.
- Inform the School Office.

Photographs and Video

Photographs and video (images) form an essential part of our teaching and learning process.

- Record images only using school equipment; your classroom camera or a school tablet.
- Evaluate images to ensure that the subjects are not portrayed in ways that may reasonably be considered embarrassing or compromising. Immediately delete any that do so.
- Transfer images from the device to designated secure storage on our network (G:\Photos and Videos) or into approved third-party applications, specifically: OneDrive, Tapestry and IRIS.
- Before images are shared to public places (display boards, local press, the school website, etc.), check for any learners who have not given consent to have their images shared. Do not share any such images.

Images stored in G:\Photos and Videos will be backed up and stored for a limited time before being fully and completely deleted from our systems. Images transferred to third-party applications will be similarly treated using appropriate features available within those systems.

The Internet

Staff and learners are encouraged to explore the internet and use a range of resources for teaching and learning. This should be done in a responsible way, open to new ideas and new ways of thinking.

Rules about internet use apply equally to all staff and learners. This helps to promote shared values within the school, and to promote shared learning.

Use of the internet is monitored by our SMOOTWALL (see Monitoring).

Network filtering is in place to prevent access to inappropriate sites, and there is keyword logging software that flags certain terms. You will see a message from Smoothwall if you have used a search term or location that may be inappropriate, or if your access to a site or resource is blocked. In most cases this will be the result of necessary over-caution on the part of Smoothwall filters or because of advertisement blocking. However, if your search term might be misconstrued as inappropriate, please make a note of what happened, as you may be asked to explain to a teacher or senior manager.

Please notify a teacher and the IT Support as soon as possible if you access any inappropriate sites by accident, or if you find inappropriate content on a workstation or the internet. Do not draw pupils' attention to the content that you have found.

You must use the internet in accordance with UK law. Any illegal use will be dealt with through official channels, which may include the involvement of police if a crime has been committed.

Email

The school provides staff with an email account as part of Microsoft Office 365. It allows us to communicate quickly with one another, and to provide a quick and easy way to deal with outside agencies on any school business.

Use of email is subject to monitoring for security and network management reasons (see Monitoring).

Staff should not email school files or documents to personal email accounts. To do work at home or at another site, use your school Office 365 account. Likewise, your school email address should only be used for school business, and in connection with teaching and learning. This applies to the use of your school email address to subscribe to online services. For example, you should not create a personal Twitter account using your school email address.

It is unacceptable to use the email system to send or receive any material that is obscene or defamatory, or to use it in any way intended to annoy, harass or intimidate another person. Any reporting instances of using email in this way will be dealt with by senior leaders.

Our Office 365 email system will append an additional section to the end of emails sent outside the organisation. This section has content determined by the School Office and implemented by IT Support. It may change from time to time but will include the school address and telephone number. When mailing external addresses conclude with an appropriate formal signature including both your name and job title. For example:

> Kind regards,
>
> Ms Joanne Bloggs.
> Teacher

Email Security

Norton CP School has strong email and internet security in place (see Monitoring and Protection). However there is always the risk that scam, phishing or chain emails may get through this, and be received on your school email account. Staff and learners need to be aware that not everything sent to your school email account may be what it seems.

Scam or phishing emails may contain nasties such as viruses, malware and ransomware. Viruses infect your machine and make it harder to use, for example by making you unable to open programs, or changing your default internet log-in page to a scam site. Malware may track information such as your web visits and key strokes, and send this back to the scammer. This may allow them to access your online accounts. Ransomware encrypts files on your machine and locks them down. When you try to open them, you see a ransom demand to have them decrypted and returned to you.

If you receive an unusual or suspicious email, do the following:

1. Do **not** open it. Do **not** forward it to anyone.
2. Write down the details that you can see without opening it (e.g. subject and sender).
3. **Permanently** delete it, thus:
   a. Delete it from your 'Inbox'.
   b. Go to your 'Deleted Items' folder and delete it again.
4. Notify IT Support.

Social Media

What is Social Media?

Social media is a general term that describes a wide variety of interpersonal applications enabled by the internet and mobile devices. Services are usually free and the providers make money by advertising and collecting personal data. Services usually offer some form of direct messaging between users and the ability to post text, images and video to friends and the wider internet community. Social media providers often conduct very little moderation of content or regulation of user registrations.

This policy applies to all forms of social media, including those that may emerge in the future.

Do We Use Social Media at Norton Community Primary School?

NCPS welcomes and encourages active communication between parents, staff, governors and the wider community. We maintain a lively website and regularly update it with articles on current events, advice for parents and activities for children to engage in outside school.

Children are encouraged to write for the website and, where permission has been given by parents, are featured in photographs and video. When used this way, the website is similar to the local press as a means to promote and remember our events and celebrate our achievements. It does not provide an interactive service whereby individuals can respond and comment on articles or content.

NCPS may use, from time-to-time, a variety of different social media technologies in order to keep everyone up-to-date with school life. Wherever possible, NCPS will strive to manage such services so that members of staff do not become bogged down moderating and responding to messages from a range of different sources. We always prefer to answer your questions or deal with issues in person. Come and see us!

Pupils

NCPS pupils have regular E-Safety lessons and are made aware that the internet, as well as being a wonderful learning resource, is also an area of risk. Pupils are taught how to keep themselves safe online and to understand the pros and cons of using online services.

Many social media services explicitly exclude primary school age children and the school will remind pupils of these restrictions on a regular basis. In practice, the social media providers are not good at preventing children from using their services. Therefore, the school will work with children to promote and encourage sensible behaviour, engaging Pupil Voice in each academic year to create a relevant and up-to-date guide for pupils.

Staff

<u>Expectations</u>

All qualified teachers in England follow rigorous standards set out by the Department for Education (DfE). These include standards for personal and professional conduct. All other members of staff are regularly briefed by the Senior Leadership Team as to Norton Community Primary School's expectations when using social media.

If members of staff have private social media accounts, they are expected to use them responsibly and be mindful of their professional status. In particular, staff members must be aware that safeguarding and maintaining confidentiality are paramount.

Should members of staff fall below these standards then the school's disciplinary procedure will be implemented. The ultimate sanction is dismissal and, for teachers, loss of Qualified Teacher Status.

<u>Keeping Children Safe</u>

Members of staff should protect themselves by declining 'friend requests' from pupils who make contact using social media. Similarly, they must not make such requests to pupils nor elect to 'follow' pupils. Staff should bear in mind the following points if they choose to include parents and other members of staff in their social media groups.

The school should not and does not attempt to remove freedom of speech and self-expression from members of staff who may wish to use social media. Staff must, however, be cautious about what they share and be aware that their responsibility to respect privacy and protect personal data applies online just as it does in print and in person.

- Staff should recognise their status as a role model for the local community and behave accordingly on social media.
- Staff must not name or identify children, discuss children's character and/or academic progress or any incident that has occurred that relates to school.
- Staff must not make derogatory comments about pupils, parents or members of staff.

<u>Keeping Staff Safe</u>

Members of staff who use social media are potentially vulnerable to malicious and defamatory comments, threats and abuse from parents or pupils, and to allegations of grooming and other forms of online abuse.

The school takes this extremely seriously and will act accordingly, as follows:

- Staff shall report instances of malicious and defamatory comments, threats and abuse to the Head Teacher.
- Staff shall not respond to messages of this nature but should flag them to the social media provider in whichever way is available on that service. For example, by using a 'Flag as abuse' feature.
- Staff should keep copies of such messages, which will be passed to the police.

Parents

The school has no desire to control or interfere in the social media activities of parents. The purpose of this policy is to make parents aware of how their online activities can affect children’s experiences both at school and in the community.

Keeping Children Safe

Many of parents’ proudest moments take place within the school walls, and it's natural to want to share photos and videos on social media. Parents should be aware that the internet is not always a safe or private place, and 'oversharing' could potentially put their own children and those of others at risk. For example, sharing photos, videos or other information can make children identifiable to others and provide confidential information that could be used maliciously.

Disputes and Grievances

Some parents may use social media to make reference to grievances they have with the school. The school will not become involved, or respond, other than to refer parents to the school’s official Complaints Procedure which should be used in such cases.

If malicious and defamatory comments or threats and abuse are made they will be treated as follows:

- The school will not respond to messages of this nature but will flag them to the social media provider in whichever way is available on that service.
- The school will keep copies of such messages, which will be passed to the police.