St Neot's Prep School

Policy Name:	**IT & E-Safety Policy**
Policy Number:	**A11**

Staff member responsible	**Revision Date**	**Approved By**	**Approval Date**	**Reason**
Alison Watt (Head of Computing) & Harriet Cairns (Operations Manager)	January 2023	Jonathan Slot (Head) & Safety and Wellbeing Governor meeting	May 2023	Annual update
Alison Watt (Head of Computing) & Harriet Cairns (Operations Manager) Bronwyn Kidd (DSL)	December 2023	Jonathan Slot (Head) & Safety and Wellbeing Governor meeting (Spring 1)	February 2023	Annual update

This policy is applicable to the whole school including Early Years

A11

Summary of changes and reviews

Version	Date	Summary	Changes by
v 1.1	Oct 22	Update ownership	HCC
V1.2	Jan 23	Review and add monitoring and filtering	HCC & BK
v1.3	November 2023	Addition of clearer outlines regarding Securly software	BK
v1.4	February 2024	Use of Mobile Phones personal devices (inc. wearable technology, mobile phones and cameras) with imaging and sharing capabilities are used in the EYFS settings	BK

Shaping Brighter Futures

We provide an inspiring and joyful education that will be remembered for a lifetime and which empowers our children with the confidence, knowledge, skills and character to thrive. We are shaping brighter futures.

School Aims:

At St Neot's education is full of fun and good humour. We want every child to enjoy their time at school, to feel part of a community that holds family values at the core. We are determined that our children not only learn outdoors but learn about the outdoors. We want to create well-rounded, independent thinkers that are not only confident in their academic ability but hold the soft skills necessary for Senior School and the world ahead.

The St Neot's Way is:

- *Where we promote a true sense of community, family values, a love of the outdoors and a commitment to having fun.*
- *Where every child comes into school feeling safe, valued and with a broad smile on their face; and who returns home with uplifting stories to tell.*
- *Where a first class, personalised, rigorous academic journey is matched by an enriching, broad and challenging co-curricular programme.*
- *Where the children's character, contribution and service is as valued as their academic success.*
- *Where the children's physical wellbeing is surpassed by their mental wellbeing.*
- *Where highly skilled, passionate and dedicated teachers, working in first class facilities, are full of ambition for themselves and the children in their care.*

St Neot's Values

Happiness Kindness Self-Belief Honesty Respect

It is the duty of St Neot's Prep School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people.

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2024 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside our Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

Introduction

Our pupils are taught how to stay safe in the online environment and how to mitigate risks, including, but not limited to, the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites (including YouTube);
- Email and instant messaging;
- Blogs;
- Social networking sites and apps (including Snapchat, TikTok, Whatsapp, Instagram);
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Mobile internet devices such as smartphones and tablets.

During the school day, pupils have access to Chromebooks and desktops. Tablets are also available for those in the Pre-Prep. All devices run through our filtering and monitoring system, Securly. Children are not allowed access to their personal devices, including mobile phones, when on the school premises.

As a school, we recognise that there are online risks that could challenge our community, examples could include:

- Cyber-bullying (typically, malicious messages or images sent via email, social media and messaging services such as Whatsapp, Snapchat or Instagram.)
    - Text messages that are threatening or cause discomfort
    - Picture/video clips via mobile phone cameras (images sent to others to make the victim feel threatened or embarrassed.)
    - Mobile phone calls (silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.)
    - Emails (threatening or bullying emails, often sent using a pseudonym or someone else's name.)
    - Chat room bullying (menacing or upsetting responses to children or young people when they are in a web-based chat room.)
    - Instant Messaging (unpleasant messages sent while children or young people conduct real time conversations online using social media, gaming websites etc.)
    - Bullying via websites (use of defamatory blogs, personal websites and online personal 'own web space' sites.)

  - Sexting (sharing of explicit images or Youth Produced Sexual Images) and/or the internet. This includes the use of images as 'revenge' when a relationship breaks down.
- Potential exposure to inappropriate and/or adult material.
- Illegal behaviour (including hacking, spamming or viewing/downloading pirated media/games, easy access to gambling platforms.)
- Inappropriate content and titles of WhatsApp groups.
- Potential exposure to predators posing as peers.
- Downloading malware, viruses, Trojans, trackers/loggers that are packaged anonymously within software, apps or web pop-ups.
- Using proxy or VPN services to purposely bypass the filtering services.
- Fake account creation – on any platform that purports affiliation or interacts with the College is not permitted. This includes using someone else's account without permission and posting offensive content pretending to be someone else.

Self-generative artificial intelligence has been a significant change, with students having often unfettered access to tools that generate text and images at home or in school. These tools not only represent a challenge in terms of accuracy when young people are genuinely looking for information, but also in terms of plagiarism for teachers and above all safety: none of the mainstream tools have end-user safety settings, most have an age limit of 13 or even 18 and in spite of basic rude words not delivering results, will easily produce inappropriate material. As a school, we recognise that we not only need to tackle this in terms of what comes into school but also educating young people and their parents on use of these tools in the home.

Against this background, the Ofcom 'Children and parents: media use and attitudes report 2023' has shown that YouTube remains the most used site or app among all under 18s and the reach of WhatsApp, TikTok and Snapchat increased yet further. As a school we recognise that many of our children and young people are on these apps regardless of age limits, which are often misunderstood or ignored. We therefore remember to remind all about best practice while remembering the reality for most of our students is quite different. In the past year, more and more children and young people used apps such as snapchat as their source of news and information, with little attention paid to the veracity of influencers sharing news. The 2023 Revealing-Reality: Anti-social-Media Report highlights that this content is interspersed with highly regular exposure to disturbing, graphic and illegal content such as fights, attacks, sexual acts and weapons. At the same time, the Children's Commissioner revealed that younger children are regularly consuming pornography and living out inappropriate behaviour and relationships due to 'learning from' pornography. This has coincided with the rise of misogynistic influencers such as Andrew Tate, which had a significant influence on many young boys over the past year which schools have had to counter.

At St Neot's School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

This policy, supported by the Acceptable Use policy, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding;
- Staff Code of Conduct;
- Health and Safety;
- Behaviour;
- Anti-Bullying;
- Acceptable Use Policy for Pupils;
- Data Protection

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and business staff, governors, and regular volunteers. 'Parents includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the Acceptable Use Policy cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

Roles and responsibilities

This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

In 2023/2024, it is vital that all members understand their responsibilities and those of others when it comes to filtering and monitoring. All staff have a key role to play in feeding back on potential issues.

1. The Governing Body
   The governing body of the school is responsible for the approval of this policy and for reviewing its effectiveness. The governing body will review this policy at least annually.

   The Headmaster is responsible for the safety of the members of the school community and this includes responsibility for e-safety. The Headmaster has delegated day-to-day responsibility to the Safeguarding Lead.

   In particular, the role of the Headmaster and the Senior Leadership team is to ensure that:
   a. staff, in particular the Safeguarding Leads are adequately trained about e-safety; and
   b. staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the school.

2. Designated Safeguarding Lead (DSL)
   The School's Safeguarding Lead is responsible to the Headmaster for the day to day issues relating to e-safety. The Safeguarding Lead has responsibility for ensuring this policy is upheld by all members of the school community, and works with IT staff to achieve this. They will keep up to date on current e-safety issues and guidance issued by relevant organisations, the DfE, including KCSIE (2024), the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

3. IT staff
   The school's technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and business staff in the use of IT. They can monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the DSL and/or Headmaster.

4. Teaching and business staff
   All staff are required to sign the Staff Acceptable Use Policy before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

5. Pupils
   Pupils are responsible for using the school IT systems in accordance with the Pupil Acceptable Use Policy, and for letting staff know if they see IT systems being misused.

6. Parents and carers
   St Neot's Prep School believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

Parents and carers are responsible for endorsing the school policy.

Handling safeguarding concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing and PSHE/RSE).

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem. All concerns must also be logged on the schools safeguarding platform; CPOMS.

St Neot's commits to take all reasonable precautions to ensure safeguarding pupils online, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the designated safeguarding lead on the same day – where clearly urgent, it will be prioritised.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2022 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 32-34 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

Sexting - sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school DSL will in turn use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved. It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child on child abuse pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying, including incidents that take place outside school or from home should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

Child-on-child sexual violence and sexual harassment

Part 5 of Keeping Children Safe in Education covers 'Child-on-child sexual violence and sexual harassment' and it would be useful for all staff to be aware of many aspects outlined there to support a whole-school response; case studies are also helpful for training.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

In the online environment, the recent proliferation of misogynistic content is particularly relevant when it comes to considering reasons for and how to combat this kind of behaviour.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy, as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the school community. These are also governed by school Acceptable Use.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, St Neot's will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Data protection and cybersecurity

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy. It is important to remember that there is a close relationship between both data protection and cybersecurity and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cybersecurity.

Schools should remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in Data protection in schools, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2024, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Filtering and Monitoring

Keeping Children Safe in Education has long asked schools to ensure "appropriate" web filtering and monitoring systems which keep children safe online but do not "overblock".

Since KCSIE 2023, in recognition of the importance of these systems to keeping children safe, the designated safeguarding lead now has lead responsibility for filtering and monitoring.

Schools are also asked to follow the new DfE filtering and monitoring standards, which require them to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

All staff need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking. They can submit concerns at any point via the Head of Computing, Operations Manager, DSL or IT Technician and will be asked for feedback at the time of the regular checks which will now take place.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via regular training reminders in the light of the annual review and regular checks that will be carried out.

At St Neot's Prep:

- Web filtering is provided by Securly web-filtering solutions on our school site and for school Google Accounts and devices used in the home.
- Changes can be made by our Head of Computing (Alison Watt) and IT Technician
- Overall responsibility is held by the DSL with further SLT support from the Operations Manager (Harriet Cairns)
- Technical support and advice, setup and configuration are from the IT Technician (Dean Hucklesbury)
- an annual review is carried out as part of the online safety audit to ensure a whole school approach

Securly Aware sends alerts between 8:00 and 18:00, however it does keep logs that can be reviewed over a 24/7 time period. Filtering remains in place 24/7 (including at home, when on their school account)

According to the DfE standards, "a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices. At St Neot's we make use of:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software, when using desktops in the IT suite (software: NetOp)
- network monitoring using log files of internet traffic and web access, via Securly
- individual account monitoring through software or third-party services, via Securly

<u>Messaging/commenting systems (incl. email, learning platforms & more)</u>

Authorised systems

Pupils at this school communicate with each other and with staff using Google platforms, including email and Google Classroom.

Staff at this school use the email system provided by Google for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system.

Staff, in the Early Years and Pre-Prep, also use Tapestry and Class Dojo to communicate with parents. iSAMS is used to support communications between the school and parents, making use of emails and the app.

Any systems above are centrally managed and administered by the school. This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed.

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from or data being uploaded to the wrong account. If this a private account is used for communication or to store data by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Behaviour / usage principles

- More detail for all the points below are given in the Social media section of this policy as well as the school's acceptable use agreements, behaviour policy and staff code of conduct
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy and only using the authorised systems mentioned above.
- Pupils and staff are not allowed to use the email system for personal use and should be aware that all use is monitored and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination (and will be dealt with according to the appropriate policy and procedure).

Online storage or learning platforms

All the principles outlined above also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc.

For all these, it is important to consider data protection and cybersecurity before adopting such a platform or service and at all times when using it. St Neot's Prep has a clear cybersecurity and data protection policy which staff, governors and volunteers must follow at all times.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headmaster and Governors have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations to the marketing manager and Deputy Head..

The site is managed by the Head of Marketing and hosted by SquareSpace.

Where staff submit information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been

fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. There are many open-access libraries of public-domain images/sounds etc that can be used. Finding something on Google or YouTube does not mean that copyright has been respected. If in doubt, check with the Operations Manager.

Digital images and video

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- I give permission for the school to take and use images and video of my child for all purposes.
- I give permission for the school to take and use images and video of my child for all purposes, excluding for use on social media.
- I give permission for the school to take and use images and video of my child for all purposes, excluding for use on social media & external marketing, which includes the school website but not the parent portal.
- I give permission for the school to take and use images and video of my child for educational purposes and Neot's News, only.
- I wish to opt out of my child's image being used, bar for the schools education purposes, as outlined above.

The above is supported by our Image Policy and E-Safety policy. Separate permissions will be gained for trips and some specific events, such as school photography via external providers.

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy. At St Neot's Prep, no member of staff will ever use their personal phone to capture photos or videos of pupils. Photos are stored on School managed & maintained devices and backed up to the cloud via Google Drive & Google Photos in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded regularly about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social media

St Neot's works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first Googling the school.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

The school Marketing Manager is responsible for managing our Instagram, Facebook and other social media accounts and checking our Wikipedia and Google reviews and other mentions online.

Staff, pupils' and parents' Social Media presence

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school regularly deals with issues arising on social media involving pupils/students under the age of 13. We

ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to refer to the Digital Family Agreement to help establish shared expectations and the Top Tips for Parents poster along with relevant items and support available from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

Although the school has an official Facebook and Instagram account and will respond to general enquiries about the school, it asks parents/carers not to use these channels for communication with the school, especially not to communicate about their children.

Email is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use. The school also currently makes use of Tapestry and ClassDojo for our Nursery and Pre-Prep children. Pupils are not allowed to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headmaster, and should be declared upon entry of the pupil or staff member to the school.

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headmaster (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there has been a significant number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital images and video [this links to the section in this document] and permission is sought before uploading photographs, videos or any other information about other people.

Device usage

AUPs remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague.

Personal devices including wearable technology and bring your own device (BYOD)

Pupils are not allowed to bring mobile phones. If they need to, they must be handed in at the school office on entry and can sign them out when going home. Any attempt to use a phone in school or to take illicit photographs or videos will lead to sanctions as per the Behaviour policy. This will be seen as a serious breach of behaviour expectations. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.

All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the 'Digital images and video' section of this document and the school data protection cybersecurity policies. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.

Volunteers, contractors, governors should leave their phones packed away and on silent. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Operations Manager should be sought and this should be done in the presence of a member staff.

Parents are asked to leave their phones in their pockets and on silent when they are on site. There are specific areas where the use of personal devices is banned, including the EYFS areas, swimming pool and changing rooms. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document on page.

Use of Mobile Phones personal devices (inc. wearable technology, mobile phones and cameras) with imaging and sharing capabilities are used in the EYFS settings

Reference and consideration has been given to: Safeguarding children and protecting professionals in early years settings: online safety considerations for managers

and the Early years foundation stage statutory framework - GOV.UK

In the EYFS, the use of personal mobile phones, devices or cameras is prohibited. EYFS staff are asked not to bring their mobile phones/devices into the classrooms. Mobiles should be locked away either in a locker or the office. If any other staff are visiting these areas, they are reminded that personal mobile phones/ devices should not be brought into the building. If this is unavoidable, they must be handed to the EYFS staff so they can be secured in the office.

In recent years an increase in wearable technology for personal fitness tracking has led to a rise in the use of smart watches. St Neot's encourages staff to take care of their physical and mental wellbeing and staff are permitted to wear such devices within the EYFS setting for the purposes of fitness tracking. When staff are child facing, devices that have messaging and sharing capabilities (such as Apple Watches) must be switched to 'aeroplane mode' which still permits step counting and telling the time. No wearable devices with imaging capabilities are permitted to be worn and must be removed and stored in a locker or office.

Misuse of personal devices will result in an escalation of disciplinary action in line with the staff code of conduct (SG7).

Signs are displayed on the entry doors informing staff, parents and visitors that mobile phones/devices are not permitted in these areas. If parents are collecting or dropping off they are asked to leave their phones/ devices in their vehicles or if this is not possible they are asked to hand them to staff so they can be secured in the office.

Official mobile phones are available for staff to use during lessons, school trips, breaktimes, Forest School and other outdoor activities for photography and emergency contact purposes only. Please make sure that the correct consent has been obtained before taking photos of pupils. Images are checked half termly by the Director of Marketing and Admissions, on every handset and images are routinely deleted. If there are any concerns relating to images that are stored or uploaded, the DSL is immediately made aware.

Use of school devices

Staff and pupils are expected to follow the terms of the school acceptable use policies for appropriate use and behaviour when on school devices, whether on site or at home.

School devices are not to be used in any way which contravenes AUPs, behaviour policy / staff code of conduct.

Wifi is accessible for visitors, such as governors. All such use is monitored.

School devices for staff or students are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning and reasonable as well as appropriate personal use.

All and any usage of devices and/or systems and platforms may be tracked.

Trips / events away from school

For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with pupils/students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Headmaster. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Emails and our school data system will also be used to send notifications/ messages to parents.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headmaster and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Full details of the school's search procedures are available in the school Behaviour Policy.

Education and training

1. Staff: awareness and training

New staff receive information on the school's e-Safety and Acceptable Use policies as part of their induction.

All teaching staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety. All supply staff receive information about e-Safety as part of their safeguarding briefing.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

Any staff concerns must be placed on CPOMS as soon as possible. If the incident is considered urgent then they are to engage with the school's Safeguarding Lead immediately.

2. Pupils: e-Safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about e-safety within a range of curriculum areas and Computing lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, pupils are taught about their e-safety responsibilities and to look after their own online safety. From Year 6, pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the Safeguarding Lead and any member of staff at the school.

From Year 8, pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images through discussion and classroom activities.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach Safeguarding Lead as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

3. Parents

The school seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The school therefore arranges opportunities for parents to learn more about e-safety and provides signposting where needs arise.

Policy Statements

1. Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device, staff should ensure that it is locked to prevent unauthorised access.

Staff at St Neot's Prep School are permitted to bring in personal devices for their own use. The use of these devices is in their own time and out of sight of pupils.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents / carers. Under no circumstances may staff contact a pupil or parent / carer using a personal telephone number, email address, social media, or other messaging system for school matters.

Pupils

If pupils bring in mobile devices (e.g. for use during the journey to and from school), they must be handed in to Reception (switched off) at the start of the day and collected as they leave school. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology. Smartwatches (with camera and internet capabilities) are not allowed to be worn by pupils. Some fitness trackers are allowed to be worn if they cannot take or store images or access the internet.

The school has introduced the use of pupil owned Chromebooks for pupils in Year 7 and Year 8 as a teaching and learning tool and pupils are required to adhere to the Pupil Acceptable Use Policy when

using Chromebooks for school work. In particular, the Pupil Acceptable Use Policy requires pupils to ensure that their use of Chromebooks for school work complies with this policy and prohibits pupils from using Chromebooks for non-school related activities during the school day.

School Chromebooks are stored in lockable cabinets in various classrooms. Access is available via teachers / the IT Department.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the SENCO and the Director of Studies to agree how the school can appropriately support such use. The SENCO will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

2. Use of internet and email

Staff

Staff must not access personal social networking sites, personal email which is unconnected with school work from school devices, or whilst teaching / in front of pupils. Such access may only be made from staff members' own devices whilst in the staff room or away from pupils (not whilst providing supervision). Personal mobile phones are not permitted in the Early Years, bar the staff offices. They must be stored away from the classrooms at all times.

When accessed from staff members' own devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses can be monitored.

Staff must immediately report to Safeguarding Lead / IT Manager the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the IT Manager.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring St Neot's Prep School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or

- posting links to or endorsing material which is discriminatory or offensive.

At times, parents and staff may become "social media friends" due to the nature of our community. However, this should be treated with caution and professionalism at all times. Staff should never make social media contact with pupils.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer using any personal email address. The School ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils

All pupils from Year 3 - 8 are issued with their own personal school email addresses for use on our network and by remote access using a web browser. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work / assignments / research / projects. Pupils should be aware that email communications through the school network and school email addresses can be monitored.

There is strong firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work / research purposes, pupils should contact the IT team for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication to the Safeguarding Lead / IT Team / or Head of Computing.

The school expects pupils to think carefully before they post any information online,or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the Safeguarding Lead / IT Team / or Head of Computing. This must be recorded on CPOMS by the person who it is reported to.

Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on CPOMS, and will be dealt with under the school's Behaviour Management Policy.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, pupils should contact the IT team for assistance.

3. Data storage and processing

The school takes its compliance with The Data Protection Act 20181 seriously. Please refer to the Data Protection Policy and the Acceptable Use Policy for further details.

Staff and pupils are expected to save all data relating to their work to their school Google Drive Account.

Staff devices should be secured if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be secured before sending, in the rare occasion this may happen now.

No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by the IT Department.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Data Protection Officer/ IT Department/ Safeguarding Lead/ Head of Computing.

4. Password security

Pupils and staff have individual school network logins and Google Workspace accounts. Staff and pupils are regularly reminded of the need for password security.

All members of staff should:

- use a strong password usually containing eight characters or more, and containing upper and lower case letters as well as numbers
- not write passwords down
- not share passwords with other staff.

5. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

Parents / carers are welcome to take videos and digital images of their own children at school events strictly for their own personal use, unless otherwise instructed not to do so e.g. in the swimming pool area and when watching swimming galas. To respect everyone's privacy and in some cases protection, images containing incidental images of other children should not be published on blogs or social networking sites without the permission of the people identifiable in them or the permission of their parents, nor should parents comment on any activities involving other pupils in the digital / video images. See Image Policy for further information.

Staff are allowed to take digital / video images to support educational aims, but must follow this policy and the Acceptable Use Policy and EYFS Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others.

Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website (see Image Consent Form for more information).

Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

6. Misuse

St Neot's will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and/or the LSCB. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Centre. Incidents of misuse or suspected misuse must be dealt with by staff in accordance with policies and procedures (in particular the Safeguarding Policy).

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy.

7. Bring Your Own Device (BYOD)

Introduction

The school recognises that mobile technology offers valuable benefits to staff from a teaching and learning perspective and to visitors. Our school embraces this technology but requires that it is used in an acceptable and responsible way.

This section is intended to address the use by staff members and visitors to the school of non-school owned electronic devices to access the internet via the school's internet connection, to access or store school information, or to make photographs, video, or audio recordings at school. These devices include smartphones, tablets, laptops, wearable technology and any similar devices. If you are unsure whether your device is captured by this policy please check with the school's IT Department. These devices are referred to as 'mobile devices' in this policy.

Sections 7.1 - 7.3 and 7.5 apply to all school staff and to visitors to the school. The rest of the policy is only relevant to school staff.

This section is supported by the Staff Acceptable Use Policy.

BYOD statements

7.1. Use of mobile devices at the school

Personal mobile devices are not permitted to be used in the Nursery or Reception classrooms, in line with Early Years Guidance. Please see SG2 Safeguarding and Child Protection Policy (Annex 5) for further details.

Staff and visitors to the school may use their own mobile devices in the following locations:

- In the classroom with the permission of the teacher.
- In the school staff workroom, staff room, business offices or in a classroom if there are no children present and the staff member is not supervising pupils.

Staff and visitors to the school are responsible for their mobile devices at all times. The school is not responsible for the loss or theft of or damage to the mobile device or storage media on the device, e.g. removable memory card. Reception must be notified immediately of any damage, loss, or theft of a mobile device, and these incidents will be logged.

The school reserves the right to refuse staff and visitors permission to use their own mobile devices on school premises. Refusal to do so may result in being asked to leave the school.

7.2. Use of cameras and audio recording equipment

Parents and carers may take photographs, videos or audio recordings of their own children at school events for their own personal use, unless they have been instructed not to do so.

Other visitors and staff may use their own mobile devices to take photographs, video, or audio recordings in school provided they first obtain permission to take photographs, films or recordings of the relevant individuals. This includes people who might be identifiable in the background.

To respect everyone's privacy and in some cases protection, photographs, video, or audio recordings should not be published on blogs, social networking sites or in any other way without the permission of the people identifiable in them. Parents or carers should avoid commenting on activities involving pupils other than their own in photographs, video, or audio, and other visitors and staff should comment.

No one must use mobile devices to record people at times when they do not expect to be recorded, and devices must not be used that would enable a third party acting remotely to take photographs, video, or audio recordings in school. Staff must comply with the school's social media policy and anti-bullying policy when making photographs, videos, or audio recordings.

7.3. Access to the school's internet connection

The school provides a wireless network that staff and visitors may use to connect their mobile devices to the internet. Access to the wireless network is at the discretion of the school, and the school may withdraw access from anyone it considers is using the network inappropriately.

The school cannot guarantee that the wireless network is secure, and staff and visitors use it at their own risk. In particular, staff and visitors are advised not to use the wireless network for online banking or shopping.

The school is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the school's wireless network. This activity is taken at the owner's own risk and is discouraged by the school. The school will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the school's wireless network.

7.4. Access to school IT services

School staff are permitted to connect to or access the following school IT services from their mobile devices:

- the school email system - Gmail
- the school virtual learning environment - Google Workspace and Google Classroom

Staff may use the systems listed above to view school information via their mobile devices, including information about pupils. Staff must not store the information on their devices, or on cloud servers linked to their mobile devices. In some cases it may be necessary for staff to download school information to their mobile devices in order to view it (for example, to view an email attachment). Staff must delete this information from their devices as soon as they have finished viewing it.

Staff must only use the IT services listed above and any information accessed through them for work purposes. School information accessed through these services is confidential, in particular information about pupils. Staff must take all reasonable measures to prevent unauthorised access to it. Any unauthorised access to or distribution of confidential information should be reported to the school's IT team and Designated Safeguarding Lead as soon as possible.

Staff must not send school information to their personal email accounts.

If in any doubt a device user should seek clarification and permission from the school's IT team before attempting to gain access to a system for the first time. Users must follow the written procedures for connecting to the school systems.

7.5. Monitoring the use of mobile devices

The school may use technology that detects and monitors the use of mobile and other electronic or communication devices which are connected to or logged on to our wireless network or IT systems. By using a mobile device on the school's IT network, staff and visitors to the school agree to such detection and monitoring. The school's use of such technology is for the purpose of ensuring the security of its IT systems, tracking school information.

The information that the school may monitor includes (but is not limited to): the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms (including passwords), information uploaded to or downloaded from websites and school IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network. The monitoring software in the school will also report various key strokes deemed harmful and inoffensive.

Staff who receive any inappropriate content through school IT services or the school internet connection should report this to the school's IT team and Designated Safeguarding Lead as soon as possible.

7.6. Security of staff mobile devices

Staff must take all sensible measures to prevent unauthorised access to their mobile devices, including but not limited to the use of a PIN, pattern or password to be entered to unlock the device, and ensuring that the device auto-locks if inactive for a period of time.

Staff must never attempt to bypass any security controls in school systems or others' own devices.

Staff must ensure that appropriate security software is installed on their mobile devices and must keep the software and security settings up-to-date.

7.7. Compliance with Data Protection Policy

Staff compliance with this BYOD policy is an important part of the school's compliance with the UK Data Protection Act 2018. Staff must apply this BYOD policy consistently with the school's Data Protection Policy.

7.8. Support

The school takes no responsibility for supporting staff's own devices; nor has the school a responsibility for conducting annual PAT testing of personally-owned devices.

7.9. Compliance, Sanctions and Disciplinary Matters for staff

Non-compliance of this policy exposes both staff and the school to risks. If a breach of this policy occurs the school will respond immediately by issuing a verbal then written warning to the staff member. Guidance will also be offered. If steps are not taken by the individual to rectify the situation and adhere to the policy, then the mobile device in question may be confiscated and/or permission to use the device on school premises will be temporarily withdrawn. For persistent breach of this policy, the school will permanently withdraw permission to use user-owned devices in school.

7.10. Incidents and Response

The school takes any security incident involving a staff member's or visitor's personal device very seriously and will always investigate a reported incident. Loss or theft of the mobile device should be reported to Reception in the first instance. Data protection incidents should be reported immediately to the school's data protection controller, Mark Kenton.

Complaints

As with all issues of safety at St Neot's Prep School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the Safeguarding Lead in the first instance, who will liaise with

the leadership team and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of or concerns around e-safety will be recorded on CPOMS reported to the school's Designated Safeguarding Lead, Bronwyn Kidd, in accordance with the school's Safeguarding Policy.