NPAT ONLINE SAFETY AND ACCEPTABLE USE OF IT POLICY

Associated Policies:	Management of allegations against staff policy Safeguarding and child protection policy Code of conduct for staff and volunteers GDPR policy Data breach policy
Author:	Chief Finance & Operations Officer, Julie Ricketts Expert Subject Lead for Computing (NPAT), Lois Beshiri
Date Approved:	21 September 2026
Approved by:	Trust Board
Date issued:	5 October 2026
Date of Review:	October 2029
Website Inclusion	N
Version:	1.3

CONTENTS

Contents 1
Key contacts 3
Policy statement 4
Who does this policy apply to 4
Policy review arrangements 4
1. Scope of the policy 4
2. Aims 5
3. Legislation and guidance 6

Northampton Primary Academy Trust is proud to produce written materials that consider the British Dyslexia Association style guide principles.

4. Roles and responsibilities 7
5. The 4 Cs of online safety 16
6. Education and curriculum 17
7. Handling online safety concerns and incidents 18
8. Examining electrical devices 18
9. Staff using work devices outside school 19
10. Access 19
11. Misuse of school technology (devices, systems, networks or platforms) 20
12. Social media 20
13. Appropriate filtering and monitoring 22
14. Trust and school websites 23
15. Cloud platforms 23
16. Digital images and video 24
17. Personal devices and bring your own device (BYOD) policy 24
18. Network / Internet access on school devices 26
19. Visits / events away from school 26
20. Training 26
SECTION 2: ACCEPTABLE USE 27
1. What is an AUP (Acceptable Use Policy) 27
2. Why have an AUP 28
3. Aims 29
4. Appropriate and inappropriate use by staff and adults 29
5. Mobile technologies 31
6. Personal recording devices 32
7. Video and photographs 32
8. Video conferencing and webcams 32
9. Safeguarding measures 33
10. Filtering 33
11. Parents 33
12. Links to other policies 34
Appendix 1 Acceptable Use Agreement 35
Appendix 2 Online Safety Incident Flowchart 38

Appendix 3 Parent/Carer and Child Acceptable Use Agreement 40
Appendix 4 Staff Procedures Following Misuse by Staff 43
Appendix 5 Staff Procedures Following Misuse by Children and Young People . 45
Appendix 6 Online Security – Cyber Security in Schools: practical tips for everyone working in education 47

KEY CONTACTS

Key contacts for online safety at the school

Designated Safeguarding Lead (DSL)	
Name	Mrs D Archer
Telephone number	01604 409608
Email address	enquiries@ectonbrook.org.uk
IT Lead	
Name	Mrs M Norris
Telephone number	01604 411534
Email address	enquiries@ectonbrook.org.uk
Online Safety Lead	
Name	Mr N Woods
Telephone number	01604 409608
Email Address	enquiries@ectonbrook.org.uk

POLICY STATEMENT

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with Keeping Children Safe in Education, (KCSIE) and other statutory documents detailed at the end of this policy.

Northampton Primary Academy Trust (NPAT/the Trust) has a Safeguarding and Child Protection policy, which acts as the sole point of reference when managing a safeguarding concern, this includes concerns that arise from the use of technology in all forms and should be referred to alongside this policy.

WHO DOES THIS POLICY APPLY TO

This policy is intended for NPAT Central Team, school staff, supply staff, pupils, parents, Trustees, Local Governors and other volunteers.

POLICY REVIEW ARRANGEMENTS

This policy will be reviewed and updated as necessary if/when any changes are made to legislation that affect our Trust's practice. Otherwise, or from then on, this policy will be reviewed every three years.

1. SCOPE OF THE POLICY

Online safety is an integral part of safeguarding.

We believe that:

- children and young people should never experience abuse of any kind
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- the online world provides everyone with many opportunities; however, it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using NPAT network and devices
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

Accordingly, this policy is written in line with Keeping Children Safe in Education (KCSIE), DfE and other statutory documents detailed at the end of this policy and recognises the online safety risks known as the **4 Cs of online safety:**

- **Content**
- **Contact**
- **Conduct**
- **Commerce**

The Safeguarding Trustee and Chief Executive Officer (as Safeguarding lead) have strategic oversight of our online safety strategy, however each of the Trust's individual school designated safeguarding leads (DSL) take lead responsibility for safeguarding and child protection (including online safety) within schools. Each school has a named Online Safety Lead (OSL). In some schools this position may be covered by the DSL as part of their remit. The OSLs can be contacted through their respective school office.

2. AIMS

Northampton Primary Academy Trusts aims to:

- have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- deliver an effective approach to online safety, which empowers the Trust to protect and educate the whole school community in its use of technology
- establish clear processes to identify, intervene and escalate an incident, where appropriate

- set out expectations for all NPAT community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- facilitate the safe, responsible and respectful use of technology to support teaching & learning
- increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- help Trust staff working with children to understand their roles and responsibilities and therefore to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care
    - for their own protection, minimising misplaced or malicious allegations
    - to better understand their own standards and practice for the benefit of NPAT and the school,
    - to support NPAT and school ethos's, aims and objectives
    - to protect the reputation of NPAT and the school
    - to establish clear structures by which online misdemeanours will be treated and procedures to follow where there are doubts or concerns (with reference to other individual school policies such as Behaviour Policy or Anti-Bullying Policy).

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account.

3. LEGISLATION AND GUIDANCE

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England.

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education (KCSIE), and the documents referenced therein.

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

This policy complies with our funding agreement and articles of association.

4. ROLES AND RESPONSIBILITIES

a) The Board of Trustees and Local Governing Bodies

The Board of Trustees has overall responsibility for monitoring this policy and holding the CEO/Headteachers to account for its implementation. The Local Governing Bodies are responsible for monitoring and the implementation of this policy at a local school level; they will also co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL)/Online Safety Lead (OSL).

All Trustees and Local Governing Body Members will:

- ensure that they have read and understand this policy
- agree and adhere to the terms on acceptable use of NPAT's ICT systems and the internet.

Governors must ensure that e-Safety is embedded within all safeguarding training, guidance and practices.

An e-Safety Governor (who may in many cases also be the nominated Safeguarding Governor) has been elected to challenge the school about:

- firewalls
- anti-virus and anti-spyware software
- filters
- using an accredited ISP (Internet Service Provider)
- awareness of wireless technology issues
- clear policies on using personal devices
- procedures for misuse, allegations or dealing with e-Safety incidents.

b) The CEO/Headteachers

The CEO/Headteachers are responsible for ensuring that staff understand this policy and that it is being implemented consistently throughout NPAT and their individual schools.

CEO key responsibilities are to:

- foster a culture of safeguarding where online safety is fully integrated into Trust-wide/whole school safeguarding
- review and update this policy (in harmony with policies for Safeguarding prevent and others) and submit for review to the Trust Board
- ensure Trustees are regularly updated on the nature and effectiveness of NPAT arrangements for online safety.

Headteacher key responsibilities are to:

- oversee the activities of the Designated Safeguarding/Online Safety Leads and ensure that the DSL and OSL responsibilities listed in the sections below are being followed and fully supported. Where the OSL is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- ensure that policies and procedures are followed by all staff
- undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Children Partnership advice
- liaise with the DSL on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- take overall responsibility for data management and information security ensuring the school follows best practice in information handling work with the DPO, DSL, Trustees and Local Governors to ensure a GDPR-compliant framework for storing data but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information
- ensure that the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles

- understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- ensure Local Governors are regularly updated on the nature and effectiveness of school arrangements for online safety
- ensure the school website meets statutory DfE requirements (see appendices for website audit document)
- ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school's individual Behaviour Policy.

c) The Designated Safeguarding Lead (DSL)/Online Safety Lead (OSL)

Details of the Designated Safeguarding Lead role (DSL) are set out in the NPAT Safeguarding & Child Protection Policy which is personalised to each school. The DSL takes lead responsibility for online safety in each school, but the management of Online Safety issues can be covered by a separate role of an Online Safety Lead (OSL) who reports to the DSL. Online Safety Lead (OSL) key responsibilities are to:

- support the CEO/Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout their school
- work with the CEO/Headteacher, IT Lead and other staff, as necessary, to address any online safety issues or incidents
- ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school's own Behaviour Policy
- update and deliver staff training on online safety with IT Lead
- liaise with other agencies and/or external services when necessary
- provide regular reports on online safety in school to Headteacher and/or Local Governors
- ensure an effective approach to online safety that empowers the school to protect and educate the whole school in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate
- liaise with the local authority and work with other agencies in line with Working together to safeguard children
- take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- work with the DPO, Safeguarding Trustee, Headteacher and Local Governors to ensure a GDPR-compliant framework for storing data but helping to ensure

that child protection is always put first, and data-protection processes support careful and legal sharing of information

- stay up to date with the latest trends and developments in online safety
- receive regular updates in online safety issues and legislation, be aware of local and school trends
- ensure that online safety education is embedded across the curriculum and beyond, in wider school life
- promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- liaise with school technical, pastoral, and support staff as appropriate
- communicate regularly with the Senior Leadership Team and the Safeguarding Governor to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how well filtering and monitoring are working
- ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- oversee and discuss 'appropriate filtering and monitoring' with Trustees and Local Governors and ensure staff are aware
- facilitate training and advice for all staff.

This list is not intended to be exhaustive.

d) The Trust IT Supplier

The Trust IT Supplier is responsible for:

- putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- ensuring that the Trust's school ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- conducting a full security check and monitoring the Trust's school ICT systems on a monthly basis
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.

e) The School IT Lead

The School IT Lead is responsible for:

- keeping up to date with the Trust's online safety policy and technical information in order to effectively carry out their online safety role and informing and updating others as relevant
- working closely with the Designated Safeguarding Lead / Online Safety Lead / Data Protection Officer to ensure that Trust systems and networks reflect NPAT policy
- ensuring the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.)
- supporting and advising on the implementation of 'appropriate filtering and monitoring' as decided by the Trust IT supplier
- maintaining up-to-date documentation of the Trust's online security and technical procedures
- Reporting online-safety related issues that come to their attention in line with NPAT policies
- manage the Trust's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack that have adequate protection, encryption and backup for data, including disaster recovery plans and auditable access controls.

This list is not intended to be exhaustive.

f) All Staff and Volunteers

All staff, including contractors, agency staff and volunteers, are responsible for:

- maintaining an understanding of this policy
- implementing this policy consistently
- agreeing and adhering to the terms on acceptable use of NPAT ICT systems and the internet (**Appendix 1**) and ensuring that pupils follow the Trust's rules on acceptable use (**Appendix 3**)
- working with their school's DSL/OSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the individual school Behaviour and/or Anti-Bullying Policy
- understanding that online safety is a core part of safeguarding; as such it is part of everyone's job – never thinking that someone else will pick it up

- knowing who the Designated Safeguarding Leads (DSL) and Online Safety Leads (OSL) are. The roles may be covered by the same member of staff.
- reading Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections)
- reading and follow this policy in conjunction with NPAT Safeguarding and Child Protection Policy
- recording online-safety incidents in the same way as any safeguarding incident and report in accordance with NPAT procedures
- understanding that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- signing and following the staff Acceptable Use Agreement and Code of Conduct
- notifying the DSL/OSL if policy does not reflect practice in your school and following escalation procedures if concerns are not promptly acted upon
- identifying opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc.) in school or setting as homework tasks, encouraging sensible use, monitoring what pupils are doing and considering potential dangers and the age appropriateness of websites
- carefully supervising and guiding pupils when engaged in learning activities that involve online technology (including, extra-curricular and extended school activities if relevant), and supporting them with search skills, critical thinking (e.g. fake news), age-appropriate materials and signposting, and legal issues such as copyright and data law
- encouraging pupils to follow their Acceptable Use Rules, reminding them about it and enforcing school sanctions
- notifying the DSL/OSL of new trends and issues before they become problems
- taking a zero-tolerance approach to bullying and low-level sexual harassment
- being aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – letting the DSL/OSL know about these
- receiving regular updates from the DSL/OSL and have a healthy curiosity for online safety issues
- modelling safe, responsible and professional behaviours in their own use of technology. This includes outside school hours and the school site, and on

social media, in all aspects upholding the reputation of the Trust and of the professional reputation of all staff

- being familiar with, or knowing where to access policies followed in school, including Safeguarding and Child Protection, Anti-bullying, Behaviour, Disciplinary Procedures and Codes of Conduct
- checking that filtering levels are appropriate for their students and are set at the correct level. Reporting any concerns about this to the OSL
- being aware of new and upcoming programmes that children are using and being aware of the age limit/risks associated with them. Regularly attending training for updates on changes to the curriculum and the requirements of teachers
- ensuring that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children and young people should know what to do in the event of an e-Safety incident
- communicating with current or past pupils, and their parents/carers, via school authorised channels only (i.e. using professional email addresses and telephone numbers). All communications with young people should be for school purposes only, unless otherwise authorised by the Headteacher, to minimise the risk of allegations being made against staff
- communicating personally (such as having social networking links) with young people currently in their care is strictly prohibited
- understanding that behaviour in their personal lives may impact upon their work with children and young people if/when shared online or via social networking sites
- ensuring that if a social networking site is used, details are not shared with children and young people and privacy settings are set to a maximum
- keeping usernames and passwords private and never leaving workstations unattended when logged in
- reporting accidental access to inappropriate materials to the OSL to allow for sites to be added to the restricted list
- being mindful of transportation of sensitive pupil/colleague information and photographs on laptops or other devices between school and home. Wherever possible, encryption or password protection should be used to restrict unauthorised access in the event of loss or theft
- addressing e-safety incidents regularly throughout the year and ensuring that sessions are planned into the curriculum to remind children of the importance of staying safe online
- planning in opportunities for children to put their knowledge of e-safety into practice.

This list is not intended to be exhaustive.

e) Pupils

Pupils are responsible for:

- reading, understanding, signing and adhering to the pupil acceptable use policy and review this when changes to the policy are made
- understanding the importance of reporting abuse, misuse or access to inappropriate materials
- knowing what action to take if they or someone they know feels worried or vulnerable when using online technology
- understanding the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realising that the NPAT Acceptable Use Policy cover actions out of school, including on social media
- understanding the benefits/opportunities and risks/dangers of the online world and knowing who to talk to at school or outside school if there are problems.

f) Parents

NPAT recognise the crucial role that parents play with regards to the safety of our pupils. Parents are therefore encouraged to:

- notify a member of staff or the individual school Headteacher of any concerns or queries regarding this policy
- ensure their child has read, understood and agreed to the terms on acceptable use of the NPAT ICT systems and internet (**Appendix 3**).

The Trust and school will raise parents' awareness of internet safety in letters or other communications home, and in information via Trust and school websites. This policy will also be shared with parents. Online safety will also be covered during parents' evenings.

Parents should:

- read, sign and promote the school's Acceptable Use Agreement and read the pupil Acceptable Use Rules and encourage their children to follow them. This should be done at the time of the child starting at the school and when changes to the policy are made
- consult with the school if they have any concerns about their children's use of technology

- promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media. For example:
    - not sharing others' images or details without permission
    - refraining from posting negative, threatening or violent comments about others, including NPAT/school staff, volunteers, governors, contractors, pupils or other parents/carers.

g) Visitors and members of the community

Visitors and members of the community who use the Trust's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

If appropriate, they will be expected to agree to the terms of acceptable use (**Appendix 1**).

External groups including parent associations

- Any external individual/organisation will sign an acceptable use agreement prior to using technology or the internet within school. It is the schools' responsibility to ensure that this happens.
- Support the Trust in promoting online safety and data protection.
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including Trust/school staff, volunteers, governors, contractors, pupils or other parents/carers.

h) Data Protection Officer (DPO)

The key responsibilities of the DPO are to:

- be aware of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (April 2018), especially this quote from the latter document:

  "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between NPAT/Schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in

the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place […]" and "Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding"

- the same document states that the retention schedule for safeguarding records may be required to be set as 'Very long-term need (until pupil is aged 25 or older)'
- work with the DSL, CEO/Headteacher, Trust Board and local governing bodies to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above
- ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

5. THE 4 CS OF ONLINE SAFETY

Keeping Children Safe in Education (KCSIE) groups online safety risks into four areas; Content, Contact, Conduct and Commerce, these are known as the 4 Cs of online safety. These have been considered in identifying potential risks and developing policy to improve and ensure online safety.

Content

Content is anything posted online - it might be words or it could be images and video. Children and young people may see illegal, inappropriate or harmful content when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Contact

Contact is about the risk of harm young people may face when interacting with other users online. This includes things like peer-to-peer pressure or seeing inappropriate commercial advertising. Sometimes adults pose as children or young adults with the intention of grooming or exploiting a child or young person for sexual, criminal, financial or other purposes.

Conduct

Conduct means the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm - for example, online bullying. Conduct also includes things like sharing or receiving nudes and semi-nude images and viewing or sending pornography.

Commerce

Commerce is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly. Schools should also consider how the risk from commerce applies to staff.

6. EDUCATION AND CURRICULUM

Each school has a Relationship, Sexual and Health Education Policy. This curriculum is bespoke to each school. The curriculum includes schemes of work around:

- Internet safety and harms
- Online relationships
- Online media
- Cyber-bullying
- Staying safe online
- Online grooming
- Sexting
- Taking care of myself online.

This list is not exhaustive.

Each school's RSHE Policy is published on their school website. The safe use of social media and the internet will also be covered in other subjects where relevant. Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc.) in any of the Trust's schools or setting of homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your individual school DSL what appropriate filtering and monitoring policies are in place). Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age-appropriate materials and signposting, and legal issues such as copyright and data law. At Northampton Primary Academy Trust, we recognise that online safety and broader digital resilience must be thread throughout the curriculum.

The following concepts, skills and competencies will be developed through both the PSHE and Computing curriculum:

- digital literacy (Online safety & behaviours)
- making good judgements about websites and emails received

- knowledge of risks such as viruses and opening mail from a stranger
- knowledge of copyright and plagiarism issues
- file-sharing and downloading illegal content
- uploading personal information – what is and is not safe
- where to go for advice and how to report abuse.

It is also the school's responsibility to plan in opportunities for children to make informed judgements and manage risks themselves rather than relying on filtering systems.

Online personal safety is taken extremely seriously within school communities and students are encouraged to refrain from sharing personal information in any form of electronic communications. Personal information includes:

- full name
- address
- telephone number
- email address.

5.2 Pupils with additional learning needs

The school strives to provide access to a broad and balanced curriculum for all learners and recognises the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness sessions and internet access.

7. HANDLING ONLINE SAFETY CONCERNS AND INCIDENTS

Safeguarding concerns will be handled in line with the NPAT Safeguarding and Child Protection Policy. The key principles of that policy, in relation to the reporting of safeguarding concerns are:

- any safeguarding concerns must be reported immediately to the Designated Safeguarding Lead
- concerns about an adult must be reported to the Headteacher, concerns about the Headteacher must be reported to the Chair of the Local Governing Body.

8. EXAMINING ELECTRICAL DEVICES

NPAT staff have the specific power under the Education and Inspections Act 2006 (as amended by the Education Act 2011) to search for and, if necessary, delete

inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, smart watches, where they believe there is a 'good reason' to do so. Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the NPAT Complaints Policy.

9. STAFF USING WORK DEVICES OUTSIDE SCHOOL

Staff members using a work device outside their place of work must not install any unauthorised software on the device and must not use the device in any way which would violate the Trust terms of acceptable use, as set out in **Appendix 1**.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside their place of work. See **Appendix 6** for more information and tips on developing and practising good Cyber Security.

The use of USB devices is not permitted by staff or students, under any circumstances.

If staff have any concerns over the security of their device, they must seek advice from the NPAT IT Service provider, or the CFOO, as soon as possible. Work devices should be used solely for work activities. If a member of staff believes their data has been shared or accessed, they must inform the Trust Data Protection Officer.

10. ACCESS

Access to the Trust's information systems and user accounts is obtained via a unique username and password. This is provided to the user by the IT Support team on the understanding that:

- any password issued to a user becomes his/her/their responsibility. No password should be shared with other users or third parties
- sharing a password may result in suspension of the user's account
- using the account of another user will result in immediate suspension of access to the Academy's/Trust's systems and referral to the Senior Leadership Team for consideration under the Trust's disciplinary procedures
- the only software authorised for use on NPAT information systems are those programs already installed on the machinery by the IT Support team or authorised for use in Trust activities. This includes online services. Any

attempt to introduce or install software onto the Academy or Trust systems will be viewed as an intention to damage NPAT property and could constitute a breach of safeguarding and/or data protection regulations, resulting in disciplinary action

- any user who causes damage, directly or indirectly, to any equipment may be refused the right to further use of the equipment and billed for its repair or replacement.

11. MISUSE OF SCHOOL TECHNOLOGY (DEVICES, SYSTEMS, NETWORKS OR PLATFORMS)

Pupils and Staff

Clear and well communicated rules and procedures are essential to govern pupil and adult use of the Trust's school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on and outside of school site). These are defined in section 2 - Acceptable Use Policy as well as in this section, for example in the sections relating to the professional and personal use of NPAT/school platforms/networks/clouds, devices and other technology.

Where pupils contravene these rules, the individual school Behaviour Policy will be applied; where staff contravene these rules, action will be taken as outlined in the NPAT Staff Code of Conduct. Further to these steps, NPAT reserves the right to monitor use of technology and/or withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto NPAT property. The school will also consider any extra-familiar harm that may be occurring, when addressing misuse of devices, systems, networks or platforms.

12. SOCIAL MEDIA

Northampton Primary Academy Trust and its constituent schools work on the principle that if we don't manage our social media reputation, someone else will. 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. Appointed staff members are responsible for managing individual schools' Facebook/Twitter etc. account(s). Breaches will be dealt with in line with the school Behaviour Policy (for pupils) or NPAT Staff Code of Conduct for staff members. Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the Trust or one of its constituent schools 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, NPAT or the school may report it to the platform it is

hosted on and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Managing social networking and other online sharing platforms

Social networking is now the communication form of choice for many adults and young people worldwide and, as a result, safeguards must be in place to ensure that staff and students are aware of the risks associated with this form of technology. To address this issue, a series of preventative measures are in place:

- Access to social networking sites is controlled through the school internet filtering systems. Teachers are to regularly monitor use and plan in opportunities for children to explore the benefits of social media within a controlled and safe environment.
- Children and staff are discouraged from providing personal details or identifiable information on profiles (e.g. mobile number, address, school name, clubs attended, email address or full names of friends). Children are asked to include images of avatars for their display icon instead of real pictures.
- Children and staff are made aware of the risks of posting images online and how publicly accessible their content is. Background images in photographs which may reveal personal details should also be addressed (e.g. house number, street name, school uniform).
- Social networking security settings should be taught, and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.
- Comments on the blogs are regularly monitored, with the teacher modelling appropriate responses which should be left.
- Both online and school systems for reporting abuse or unpleasant content, i.e. cyberbullying, are reinforced www.thinkuknow.co.uk.

Staff using social networks

Social networking outside of work hours, on non-school issue equipment, is the personal choice of all school staff. Owing to the public nature of such websites, staff have a responsibility to ensure that their actions outside of school do not impact on their work with children and young people.

Safer Recruitment Consortium's Guidance for safer working practice for those working with children and young people in education settings clearly states that adults working with children should:

- only make contact with students for professional reasons and with the authorisation of the Headteacher. Any communication should be via professional email only and never through a personal email account
- ensure that if a social networking account is used, details are not shared with children and young people and privacy settings are set to a maximum
- be aware that behaviour in their personal lives may impact on their work with children and young people
- not behave in a manner which would lead any reasonable person to question their suitability to work with children and young people.

13. APPROPRIATE FILTERING AND MONITORING

Keeping Children Safe in Education obliges schools to ensure that appropriate filters and appropriate monitoring systems are in place and that children are not able to access harmful or inappropriate material, but at the same time be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Communication

Currently across the Trust schools we use Office 365 – Outlook and Teams functions. This system is fully auditable, trackable and managed on behalf of the Trust's school. This is for the mutual protection and privacy of all Trustees, Local Governors, Staff, Pupils and parents, as well as to support data protection. Email is the main means of electronic communication to be used between staff and pupils / staff and parents (in both directions).

Communication between staff members can also take place on the Teams platform via its chat facility. Use of a different platform for communication between staff and pupils and or staff and parents must be approved by the Headteacher in advance. 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). Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the CEO/CFOO/Headteacher should be informed immediately. Staff or pupil personal data should never be sent/shared/stored on email.

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 NPAT or the school into disrepute or compromise the professionalism of staff. Staff are not allowed to use the email system for personal use. Staff should be

aware that all use is monitored, their emails may be read, 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.

14. TRUST AND SCHOOL WEBSITES

The NPAT and individual school websites are a key public-facing information portal for the school communities (both existing and prospective stakeholders) with a key reputational value. The Department for Education has determined information which must be available on a school website and the Trust annually audits the school websites to support compliance. When staff submit information for the website, they are asked to remember: NPAT has the same duty as any person or organisation to respect and uphold copyright law. Some local schools have been fined thousands of pounds for copyright breaches. Sources must always be credited, and material only used with permission. Where pupil work, images or videos are published on the website, their identities are protected, and full names are not published.

15. CLOUD PLATFORMS

The Trust and its schools adhere to the principles of the Department for Education document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'. As more and more systems move to the cloud, it becomes easier to share and access data.

When using a cloud storage solution, the following principles apply:

- Privacy statements inform parents when and what sort of data is stored in the cloud.
- The IT Lead in consultation with the CEO and Headteacher approves new cloud systems, what may or may not be stored in them and by whom.
- The DPO will ensure GDPR requirements are met when data is shared.
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such.
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen.
- Pupil images/videos are only made public with parental permission.
- Only NPAT-approved platforms are used by students or staff to store pupil work.

16. DIGITAL IMAGES AND VIDEO

When a pupil joins an NPAT school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos and for what purpose (beyond internal assessment, which does not require express consent). 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 Section 2 of this policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At any of the Trust's schools, no member of staff will ever use their personal phone to capture photos or videos of pupils. Photos are stored on the NPAT networks in line with the retention schedule of the NPAT Data Protection Policy. Pupils are discouraged from 'following' staff, Trustees, Local Governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). *Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher and should be declared upon entry of the pupil or staff member to the school).

17. PERSONAL DEVICES AND BRING YOUR OWN DEVICE (BYOD) POLICY

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.

Data protection and data security

Child/staff data should never be downloaded onto a private or personal device of any kind, including a mobile 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.

Use of mobile phones by staff - personal mobile phones

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to make or receive calls, or send texts, while children are present and during contact time. Use of personal mobile phones must be restricted to non-contact time, and to areas of the school where pupils are not present (such as the staff room). If walking to one of these places, mobile phones should not be in

use – this includes hours when breakfast or after school clubs are in operation. They must also not be used in corridors or just outside a classroom.

There may be circumstances in which it is appropriate for a member of staff to have use of their phone during contact time, for instance:

- expected emergency contact by their child, or their child's school
- expected emergency contact for acutely ill dependents or family members
- expected call back from a doctor or medical consultant
- the staff members job requires extensive lone working (such as a site manager)
- use of specific apps or programmes that are approved, by prior agreement, by the Senior Leadership Team'
- supervision of trips or residential visits.

Requests to have access to a mobile phone during times when children are present must be agreed by a member of SLT. If agreed, then any call must be taken away from pupils in designated phone safe areas and the person receiving the call must ensure their class or group is covered by another member of staff before accepting the call. If deemed necessary, school staff should use the school office number as a point of emergency contact.

Volunteers, contractors, Trustees and Local Governors should leave their phones in their pockets and on silent.

Under no circumstances should mobile phones be used in the presence of children to take photographs or videos. If this is required (e.g., for contractors to take photos of equipment or buildings), permission of the Headteacher should be sought. Photographs and/or videos should be done in the presence of a member staff.

Use of personal devices in school by children

Northampton Primary Academy Trust accepts that pupils in Years 5 and 6 who walk home alone may be provided with a mobile phone by parents for personal safety. Where mobile phones are carried by pupils in Year 5 or 6, the individual school procedures must be followed in the handling of the phone and the secure storage during school hours to ensure no access. Children who are not in Years 5 or 6 or who do not walk home alone are not permitted to bring mobile phones into Trust schools.

Smart watches are only permitted for use by pupils where these have been internet disabled by the connected smart phone being switched off.

Pupils are not permitted to bring any other digital devices into NPAT Schools.

- Digital devices may include but are not limited to: mobile communication systems and smart technologies such as Smart watches (where these are internet enabled)
- personal digital assistants (palm organisers, pocket PCs etc)
- handheld entertainment systems (video game consoles, earphones etc)
- portable internet devices (tablets, iPads etc)
- any digital device with the capacity to capture images, videos or audio (camera pens, audio recording equipment etc).

Northampton Primary Academy Trust Schools will accept no responsibility for replacing lost, stolen or damaged devices bought to school premises.

Any devices bought into school in breach of this policy, will require parents to be contacted as part of the confiscation process and sanctions applied in accordance with the individual school policy.

18. NETWORK / INTERNET ACCESS ON SCHOOL DEVICES

Pupils are not allowed networked file access via personal devices. However, they are allowed to access the school wireless internet network for school-related internet use within the framework of the Acceptable Use Rules. All such use is monitored. Child/staff data should never be downloaded onto a private phone. Volunteers, contractors (with the exception of the Trust IT supplier), Trustees and Local Governing Body Governors can access the guest wireless network but have no access to networked files/drives, subject to Section 1: Acceptable Use of this policy.

All internet traffic is monitored.

19. VISITS / EVENTS AWAY FROM SCHOOL

For school visits /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.

20. TRAINING

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

SECTION 2: ACCEPTABLE USE

1. What is an AUP (Acceptable Use Policy) 27
2. Why have an AUP 28
3. Aims 29
4. Appropriate and inappropriate use by staff and adults 29
5. Mobile technologies 31
6. Personal recording devices 32
7. Video and photographs 32
8. Video conferencing and webcams 32
9. Safeguarding measures 33
10. Filtering 33
11. Parents 33
12. Links to other policies 34

Appendix 1 Acceptable Use Agreement 35
Appendix 2 Online Safety Incident Flowchart 38
Appendix 3 Parent/Carer and Child Acceptable Use Agreement 40
Appendix 4 Staff Procedures Following Misuse by Staff 43
Appendix 5 Staff Procedures Following Misuse by Children and Young People . 45
Appendix 6 Online Security – Cyber Security in Schools: practical tips for everyone working in education 47

1. WHAT IS AN AUP (ACCEPTABLE USE POLICY)

This Acceptable Use Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all technologies to safeguard adults, children and young people within our school. The policy recognises the ever-changing nature of emerging technologies within the curriculum and media and highlights the need for regular review to incorporate development within ICT. At present the internet technologies used extensively by young people in both home and school environments include:

- school websites/blogs
- social networking
- gaming/forums on Xbox live, etc.

- music downloading
- mobile phones with wireless connectivity
- email and instant messaging
- Office 365
- Skype/Zoom/Teams
- video broadcasting
- Apple/Windows apps.

This policy provides support and guidance to parents/carers and the wider community (where appropriate) for the safe and responsible use of these technologies beyond the school or educational setting. It also explains procedures for any unacceptable use of these technologies by children or young people and refers to school disciplinary procedures for staff.

2. WHY HAVE AN AUP

The use of the internet as a tool to communicate and develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children access these technologies.

The risks include:

- spam and other inappropriate e-mail
- online grooming
- illegal activities of downloading or copying any copyright materials and file-sharing via the internet or any mobile device
- viruses
- cyberbullying
- sexting-the sending of indecent personal images, videos or text via mobile phones for private viewing
- in-line content which is abusive or pornographic
- radicalisation and other religious movements
- social and emotional effects of an increased use of technology.

It is also important that adults are clear about the procedures, for example, only contacting children and young people about homework via a school e-mail address, not a personal one, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks. Where possible, another member of staff should be copied into emails to also reduce risks. There is also a

responsibility to educate parents about the risks and how this is managed inside school, along with what they can do at home to help safeguard their child.

As part of the Education Act 2004 and the Children's Act, it is the duty of schools to ensure that children and young people are protected from potential harm both within and beyond the school environment. Every effort will be made to safeguard against all risks, however it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure children and young people continue to be protected.

3. AIMS

The aims of this policy are to:

- emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within and outside school or other educational settings.
- provide safeguards and rules for acceptable use to guide all users, whether staff or student, in their online experiences.
- ensure adults, including parents, are clear about procedures for misuse of any technologies both within and beyond the school or educational setting.
- develop links with parents/carers and the wider community ensuring input into policies and procedures.

4. APPROPRIATE AND INAPPROPRIATE USE BY STAFF AND ADULTS

To ensure that both young people and staff are appropriately safeguarded against online risks and allegations, a copy of the Online Safety Policy will be made accessible to all. The policy clearly highlights any behaviours or practices, linked to staff use of technologies, which are deemed inappropriate by Safer recruitment Consortium's Guidance for safer working practice or other relevant safeguarding legislation and professional standards. Staff are expected to take responsibility for their own use of technology and are asked to read and sign acceptance of the staff acceptable use rules annually (see **Appendix 1** for template).

Where a staff member is issued with a 'work' laptop or device this should be used solely for work-related tasks, including communication, data processing, research and project management. Personal use is not permitted.

Examples of inappropriate use:

- accepting or requesting current or past pupils as 'friends' on social networking sites or exchanging personal email addresses or mobile phone numbers.
- behaving in a manner which would lead any reasonable person to question a staff member's suitability to work with children or act as a role model. This would include inappropriate comments, photographs or videos on social networking sites which reflect badly on either the individual, their colleagues or the school/workplace.
- using a work issued device for personal use during working hours.

In the event of inappropriate use

If a member of staff is believed to misuse the internet or learning platform in an illegal, inappropriate or abusive manner, a report must be made to the Headteacher immediately and the e-Safety Incident Flowchart referred to (see **Appendix 2**). The appropriate NSCP allegation procedures and child protection policies must be followed to deal with any misconduct and all relevant authorities contacted. In the lesser event of minor or accidental misuse, internal staff disciplinary procedures will be referred to in terms of any action to be taken.

Inappropriate use by children

The pupil Acceptable Use Rules provide children with clear guidelines on appropriate use of the internet and technologies within school and are linked to school disciplinary procedures. Where appropriate, pupils sign acceptance of the rules when they join the school, and they are displayed throughout the school as a reminder.

To encourage parental/carer support of the pupil Acceptable Use Rules, a copy is sent home with the related school sanctions for misuse. This is also displayed on the school website and is clearly seen around school.

Parents/carers are asked to sign the Acceptable Use Rules with their child annually to show their support of the online safeguarding rules in place (see **Appendix 3** for template).

In the event of inappropriate use

If a child is found to be misusing online technologies or equipment whilst at school, the following sanctions will apply:

- Failure to abide by Acceptable Use Rules and deliberate misuse of the internet/technologies will result in a letter being sent home to

parents/carers explaining the reason for suspending the child's use for a particular lesson or activity.

- Further misuse of the rules may result in withdrawal of a student's internet privileges for a period of time and another letter sent home to parents/carers.
- A letter may be sent to parents/carers outlining the breach in Child Protection Policy where a child is deemed to have misused technology against another child or adult.

In the event of accidental access to inappropriate materials, children are expected to notify an adult immediately and attempt to minimise or close the content until an adult can take action.

In the event of a member of staff being aware of a child having an account for a platform that they are not legally of an age to use e.g. Facebook, Snapchat, Instagram, TikTok, a letter will be sent home to their parents informing them of this and reminding them of the legal age requirement.

Appropriate e-Safety incident procedures are then followed.

5. MOBILE TECHNOLOGIES

Everyday technologies are increasingly being used by both adults and children within the school environment. For this reason, appropriate safeguards must be in place to protect young people and staff against the following associated risks:

- Inappropriate or bullying text messages
- Images or video taken of adults or peers without permission
- Videoing violent, unpleasant or abusive acts towards a peer or adult which may be distributed
- Sexting - the sending of suggestive or sexually explicit personal images via mobile phones
- Wireless internet access which can bypass school filtering and allow access to inappropriate or potentially harmful material or communications.

All teachers have access to a school mobile device to use when taking photos. No personal devices or mobile phones should be used for this. Devices should be regularly monitored and wiped clear throughout the academic year.

6. PERSONAL RECORDING DEVICES

Users must not use ANY personal device to capture, record, stream or transmit audio, video or images on Trust premises or during Trust activities without prior authorisation.

This restriction applies to all recording technologies, including but not limited to mobile phones, tablets, smart watches, smart glasses, smart earbuds or earplugs with recording capability, wearable devices and any future technologies capable of recording or transmitting information.

Any authorised use must comply with the Trust's Data Protection, Safeguarding and Information Security requirements. Deliberate or unauthorised recording may be treated as a disciplinary matter and may result in withdrawal of IT access, disciplinary action or other appropriate sanctions.

7. VIDEO AND PHOTOGRAPHS

Images or videos featuring students will only feature on the school website or in press coverage if permission has been granted by parents/carers in advance. Wherever possible group shots of children will be taken, as opposed to images of an individual, and first names only will be displayed.

Photographs should not show children in compromising positions or in inappropriate clothing (e.g. gym kit, swimming costumes).

School equipment will be used to take any images of students, and pictures should be removed from cameras and utilised appropriately within 24 hours of being taken. This is to ensure that images of students cannot be viewed by unauthorised individuals in the event of loss or theft.

8. VIDEO CONFERENCING AND WEBCAMS

To safeguard staff and young users, publicly accessible webcams are not to be used in school. As with video and photographs, permission will be sought from parents/carers before a child engages in video conferencing with individuals or groups outside of the school setting (e.g. communicating with a school overseas). All video conferencing will be supervised by staff and a record of dates, times and participants held in school for audit trail purposes.

9. SAFEGUARDING MEASURES

Under the Counterterrorism and Security Act 2015, which came into force on 1 July 2015, there is a requirement that schools "have due regard to the need to prevent pupils being drawn into terrorism." NPAT uses software which is installed onto all child devices in the school. This software detects key words which are either typed in or appear on the screen. An image is taken of the screen and logged in the central system. The device, year group, time and content are then listed. Weekly monitoring takes place, with each 'hit' being reviewed and categorised. Any further action required is carried out by the OSL. Repeated incidents are logged to form a history if needed.

10. FILTERING

The NPAT IT Supplier provides a filtered internet service to NPAT Schools, enabling them to assign appropriate levels of access to pupils and staff depending on role, age and maturity.

10.1 Tools for bypassing filtering

Web proxies are the most popular and successful method for students to bypass internet filters in order to access unauthorised online content on the school network. A web proxy is capable of hiding the IP address of the user and opening unrestricted and, in cases, unidentifiable channels through which blocked material can be viewed e.g. social networking sites, gaming websites or adult content. To manage this safeguarding concern, students and staff are forbidden to use any technology designed to circumvent, avoid or bypass school security controls (including internet filters, antivirus solutions or firewalls). Violation of this rule by either staff or students will result in school sanctions being applied.

11. PARENTS

11.1 Roles

Each child will receive a copy of the Acceptable Use Rules on their first-time entry to the school and each time there is a change to policy. The children and their parents/carers are asked to read and sign acceptance of the pupil 'Acceptable Use Rules' to be returned to, and stored by, the school. Parents are also encouraged to attend any Online Safety workshops and visit the Online Safety section of their child's school website further understand the issues surrounding young people today and technology.

11.2 Support

As part of the school's approach to developing Online Safety awareness with children and young people, every effort is made to offer parents/carers the opportunity to find out more about how they can support their child to stay safe online within and beyond the school environment. Online Safety Parent/Carer Information Sessions will be held regularly to raise awareness of key internet safety issues and highlight safeguards currently in place at school (e.g., filtering and training in place to minimise online risk.) Free to order resources from Childnet www.childnetint.org/kia/parents/ and the Thinkuknow website www.thinkuknow.co.uk/teachers/resources/ can be used to support this. Wherever possible, the school will endeavour to provide internet access for parents/carers without this resource at home to ensure that appropriate advice and information on this topic can be viewed.

12. LINKS TO OTHER POLICIES

12.1 Behaviour, Cyberbullying and Anti-Bullying

Section 2 - Acceptable Use is cross-referenced throughout a number of other policies in place throughout the Trust and in the school, including those for behaviour, anti-bullying, PSHE and safeguarding and child protection. Cyberbullying features within schools' anti-bullying policies due to the growing number of incidents recorded. Cyberbullying will not be tolerated in or outside of school and clear procedures for dealing with cyberbullying incidents can be found within school antibullying policies.

12.2 Managing allegations and concerns of abuse made against people who work with children.

Please refer to the NPAT Management of Allegations Against Staff Policy.

12.3 School websites

Permission will be sought from parents/carers prior to the uploading of any images onto school websites. Consideration is given to what information is relevant to share with the general public on a website and secure areas will be used for information pertaining to specific audiences. The school's Acceptable Use Rules will also be published on this platform along with recommended websites.

12.4 Disciplinary Procedure for All School Based Staff

In the event that a staff member is seen to be in breach of professional standards of conduct or is believed to have misused online technologies, school disciplinary procedures and sanctions will be applied.

Appendix 1 Acceptable Use Agreement

By reading and marking this policy on Every, staff agree to abide by this Acceptable Use agreement.

APPENDIX 1
Acceptable use of the NPAT/School's ICT systems and the internet: agreement for Staff, Trustees, Local Governors, Volunteers and Visitors

ICT and the related technologies such as email, the internet and mobile phones are an expected part of our daily working life in school. This policy is designed to ensure that all Staff, Trustees, Local Governors, Volunteers and Visitors are aware of their professional responsibilities when using any form of ICT.

All Staff, Trustees, Local Governors, Volunteers and Visitors are expected to sign this policy and adhere at all times to its contents. Failure to follow this policy may result in disciplinary or other action in accordance with the NPAT/School's e-Safety policy.

- I will not engage in any activity that is illegal under UK or European law, including but not limited to:
  - Copyright Violation
  - Introducing malicious programs into the school network
  - Using school systems to download, store, or distribute illegal software and media
  - Effecting security breaches. Security breaches include but are not limited to: accessing data which I am not the intended recipient; accessing a server or account without express authorisation; enabling another to gain access to data and systems without authorisation.

- I will only use the NPAT/School's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the CEO/Headteacher, Trust Board or Local Governing Body.

- I will not install software on any NPAT/School device without authorisation.

- I will not attempt to bypass internet filtering systems or other network security systems.

- I understand that I cannot expect files stored on NPAT/School servers/platforms or equipment will always be private. Due to the need to protect the NPAT/School network's the confidentiality of information stored on any device belonging to the NPAT/School cannot be guaranteed.

- I understand that authorised individuals within the NPAT/School may monitor equipment, system and network traffic. Any unauthorised files found will be

deleted without warning and use in breach of this agreement will be reported to my line manager.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will only access the computer system with the login and password I have been given.
- I will not access other network user's files unless specifically authorized to do so.
- I will ensure that all electronic communications with Students and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any NPAT/School business.
- I will not send to Students or colleagues' material that could be considered offensive or illegal.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, or accessed remotely.
- I will not take personal or sensitive data off site on any equipment including computers and removable media unless permission is sought and appropriate encryption is used.
- I will not browse, download or upload material that could be considered offensive or illegal.
- Images of Students will only be taken and used for professional purposes and will not be distributed outside the school network without the permission of the parent/carer.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will support and promote the NPAT/School's Online Safety policy and help Students to be safe and responsible in their use of ICT and related technologies.
- I will report any accidental access to inappropriate materials to the appropriate line manager.

- I will ensure all documents are saved, accessed and deleted in accordance with the NPAT/School's network security and confidentiality protocols.

- I will not connect a computer or laptop to the NPAT/School's network / Internet that does not have up-to-date version of anti-virus software.

- I will not allow unauthorised individuals to access Email / Internet / Intranet.

- I agree and accept that any computer or laptop loaned to me by the NPAT/School, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

- I understand any personal blogging, either through NPAT/School or personal equipment, is subject to the terms and restrictions of this policy. I will not provide pupils with access to personal profiles on social networking sites or add students as "friends". I will ensure my profiles are "locked down" for my own protection.

- I will not employ any NPAT/School IT equipment for commercial purposes other than that of approved NPAT/School business.

- I will immediately report any unauthorised use of NPAT/School systems or any attempt by an individual, group or third party to breach the NPAT/School's security system, whether or not it is successful.

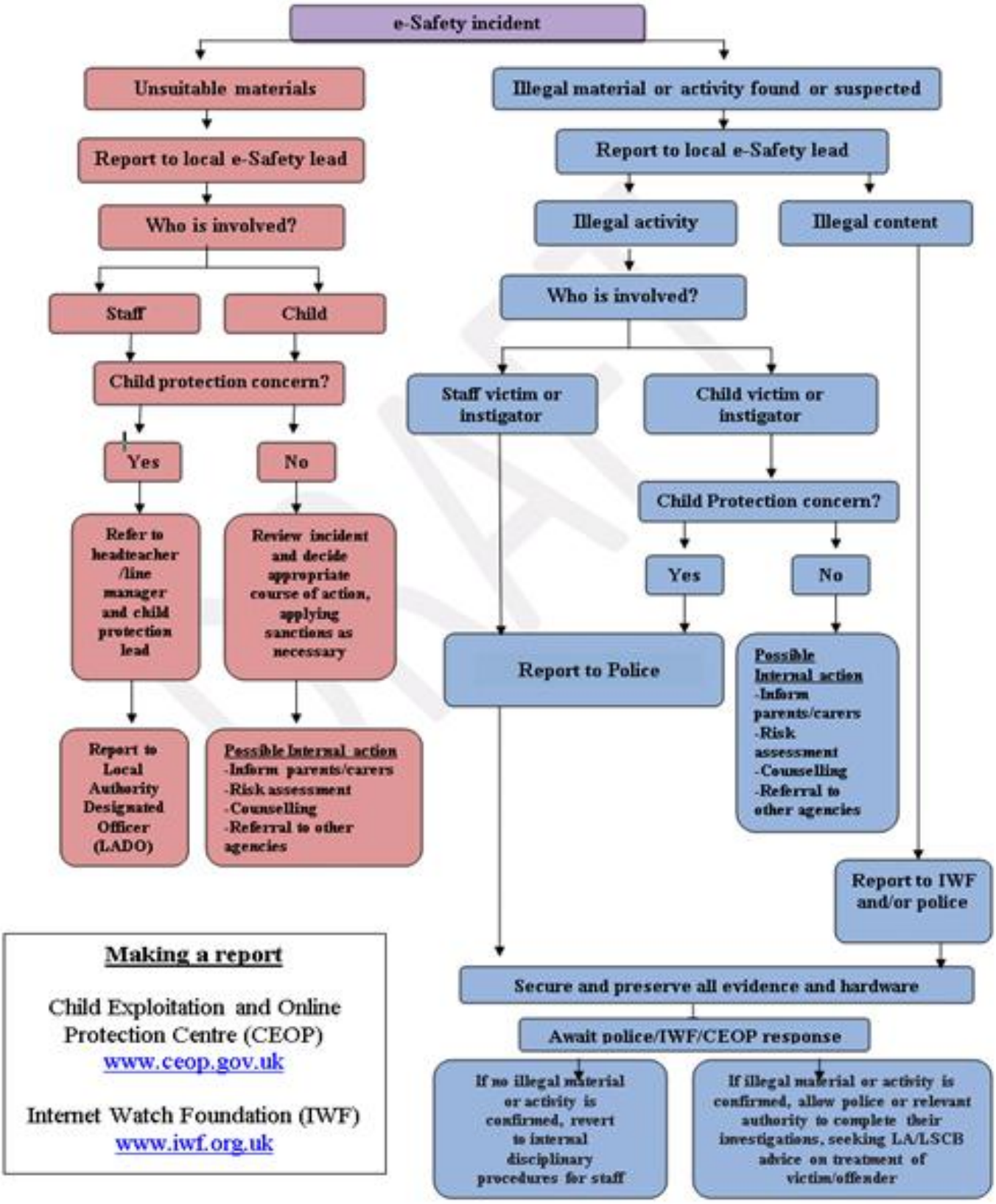
- I will protect the NPAT/School's IT equipment. Where damage or loss has occurred, I will be liable for the cost of replacement.

- I will report any faults with IT systems to the support desk using the help desk system at the earliest opportunity.

- I will not attempt to alter the configuration or setup of any IT systems without the correct authorisation.

- I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action, or referral to the police in the event of a serious breach.

Appendix 2 Online Safety Incident Flowchart



There are three instances when you must report directly to the police:

- Indecent images of children found (i.e. under 18 years of a sexual nature)
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.

If an indecent image is found CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions. The police will advise on how to deal with the machine if they are unable to send out a forensics team immediately. If in doubt, do not turn off the machine. The Internet Watch Foundation www.iwf.org.uk offers further support and advice in dealing with offensive images online. It is important to remember that any offensive images received should never be forwarded, even if it is to report them as illegal, as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Appendix 3 Parent/Carer and Child Acceptable Use Agreement

Dear Parents/Carers,

As part of an enriched curriculum, your child will be accessing the internet, school email and virtual learning environment via a filtered service provided by our IT supplier. In order to support the school in educating students about safe use of the internet, we are asking parents and children to read and sign acceptance of the attached acceptable use rules. Completed forms should be returned to the school as soon as possible.

The rules provide an opportunity for further discussions with your child about safe and appropriate use of the internet and other online tools (e.g. mobile phones), both within and beyond school (e.g. at a friend's house or at home). Sanctions in place for misuse of technologies and subsequent breach of the rules are detailed in the full Online Safety incorporating Acceptable Use Policy which parents/carers are welcome to view.

Should you wish to discuss the matter further please contact the Headteacher.

Yours faithfully,

Headteacher

Acceptable Use Rules Return Slip

Child Agreement:

Name: _____Class:_____

- I understand the rules for using the internet and email safely and responsibly.
- I know that the adults working with me at school will help me to stay safe and check that I am using the computers to help me with my work.

Child Signature: _____ Date: _____

Parent/Carer Agreement:

- I have read and discussed the rules with my child and confirm that he/she has understood what the rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the internet, email and other online tools.
- I understand that filtering can never be completely fool proof and occasionally inappropriate materials may be accessed. I accept that the school will endeavour to deal with any incident that may arise swiftly and according to policy.
- I understand that my child's safe use of the internet and online technologies outside of school is my responsibility.

Parent/Carer Signature: _____ Date: _____

Online Rules

These are our rules for using the internet safely.

Key Stage 1 Our Online Rules

- We learn how to use the internet safely.
- We can send and open messages with an adult.
- We can write polite and friendly emails or messages to people that we know.
- We only tell people our first name.
- We learn to keep our password a secret.
- We know who to ask for help.
- If we see something we do not like we know what to do.
- We know that it is important to follow the rules.
- We are able to look after each other by using the internet safely.
- We can go to www.thinkuknow.co.uk for help.

Key Stage 2 Our Online Rules

These are our rules for using the internet safely and responsibly.

- We use the internet to help us learn and we know how to use it safely and responsibly.
- We send emails and messages that are polite and friendly.
- We will only email, chat or go on webcam with people that we know in real life, with permission from our teachers or parents.
- We make sure that an adult always knows when we are online.
- We never give out passwords or personal information (like our full name, school or address).
- We never post photographs without permission and never include names with photographs.
- We know who to ask if we need help.
- If we see anything on the internet or on email that is scary or makes us feel uncomfortable, we know what to do.
- We never open emails or links from people we don't know.
- We know that the rules are there to keep us safe and must not be broken.
- We are able to keep ourselves and each other safe by using the internet in a responsible way.
- We can go to www.thinuknow.co.uk for help

Further Information and Guidance

- www.parentscentre.gov.uk (for parents/carers)
- www.ceop.co.uk (for parents/carers and adults)
- www.iwf.org.uk (for reporting of illegal images or content)

- www.thinkuknow.co.uk information and resources for children, teenagers, parents/carers and professionals
- www.netsmartzkids.org (ages 5 – 17)
- www.kidsmart.org.uk (all under 11 years old)
- www.phonebrain.org.uk (for Years 5 – 8)
- www.bbc.co.uk/cbbc/help/web/staysafe (for Years 3 - 4)
- www.hectorsworld.com (for Reception, Years 1 and 2 and is part of the *Thinkuknow* website above)
- www.education.gov.uk (for adults and professionals)
- www.digizen.org.uk (for materials from DCSF around the issue of cyberbullying)

Signed _____ Dated_____

Appendix 4 Staff Procedures Following Misuse by Staff

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by an adult:

A. **An inappropriate website is accessed inadvertently:**

Report website to the OSL if this is deemed necessary. IT lead will add this site to the banned list immediately.

B. **An inappropriate website is accessed deliberately:**

- Ensure that no one else can access the material by shutting down.
- Log the incident.
- Report to the Headteacher and OSL immediately.
- Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.

C. **An adult receives inappropriate material:**

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the Headteacher immediately.
- Ensure the device is removed and log the nature of the material.
- Contact relevant authorities for further advice e.g. police.

D. **An adult has used ICT equipment inappropriately:**
Follow the procedures for B.

E. **An adult has communicated with a child or used ICT equipment inappropriately:**

- Ensure the child is reassured and remove them from the situation immediately, if necessary.
- Report to the Headteacher and DSL immediately, who should then follow the Allegations Procedure and Child Protection Policy from Section 12, LSCBN.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Headteacher to implement appropriate sanctions.
- If illegal or inappropriate misuse is known, contact the Headteacher or Chair of Governors (if allegation is made against the Headteacher) and DSL immediately and follow the Allegations procedure and Child Protection Policy.
- Contact CEOP (Police) as necessary.

F. **Threatening or malicious comments are posted to the school website or learning platform (or printed out) about an adult in school:**

- Preserve any evidence.
- Inform the Headteacher immediately and follow Child Protection Policy as necessary.
- Inform the RBC/LA/LSCBN and OSL so that new risks can be identified.
- Contact the police or CEOP as necessary.

G. **Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted**

This should be reported to the Headteacher.

Appendix 5 Staff Procedures Following Misuse by Children and Young People

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the internet, by a child or young person:

A. **An inappropriate website is accessed inadvertently:**

- Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
- Report website to the OSL if this is deemed necessary.
- IT lead will add site to the banned list immediately.

B. **An inappropriate website is accessed deliberately:**

- Refer the child to the Acceptable Use Rules that were agreed.
- Reinforce the knowledge that it is illegal to access certain images and police can be informed.
- Decide on appropriate sanction.
- Notify the parent/carer.

C. **An adult or child has communicated with a child or used ICT equipment inappropriately:**

- Ensure the child is reassured and remove them from the situation immediately.
- Report to the Headteacher and DSL immediately.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- If illegal or inappropriate misuse the Headteacher must follow the Allegation Procedure and/or Child Protection Policy from Section 12, LSCBN.
- Contact CEOP (Police) as necessary.

D. **Threatening or malicious comments are posted to the school website or learning platform about a child in school:**

- Preserve any evidence.
- Inform the Headteacher immediately.
- Inform the RBC/LA/LSCBN and OSL so that new risks can be identified.
- Contact the Police or CEOP as necessary.

E. **Threatening or malicious comments are posted on external websites about an adult in the school or setting:**

- Preserve any evidence.
- Inform the Headteacher immediately.

N.B. There are three incidences when you must report directly to the police.

- Indecent images of children found.
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found. They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately. If in doubt, do not power down the machine.

Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image.

www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line.

Procedures need to be followed by the school within Section 12 of the Allegations Procedure and Child Protection Policy from the Local Safeguarding Children's Board Northamptonshire or Milton Keynes guidance (as appropriate).

All adults should know who the Designated Safeguarding Lead is.

It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the Police.

Appendix 6 Online Security – Cyber Security in Schools: practical tips for everyone working in education

(Source: National Cyber Security Centre: Resources for schools - NCSC.GOV.UK)

Each school needs to look after its data as well as manage the risks of using networked computers and service and so everyone needs to follow some basic principle of good cyber security.
Senior leaders and governors need to be aware that cyber security is a management and assurance issue. After all, poor cyber hygiene could affect as school's ability to function, its reputation and its legal obligations to keep personal data safe.

1. Why cyber security matters to schools

An increasing number of school and colleges are being seriously impacted by cyber incidents: perhaps a phishing attempt to steal money and passwords, or a ransomware attach that encrypts files preventing access. Why?

- Many cyber incidents are actually untargeted.
- They can affect any school that doesn't have basic levels of protection.
- Schools hold plenty of sensitive information. For example, staff and parents bank details, medical information about students, safeguarding records. All this has to be kept safe and confidential.
- Cyber criminals want to make money.
- They understand that an organisations' information is often sufficiently important to that organisation that they might be prepared to pay a ransom to get it back.

2. Who is behind cyber-attacks?

Online criminals
Online criminals Are really good at identifying what can be monetised, for example stealing and selling sensitive data, or holding systems and information to ransom.

Hackers
Individuals with varying degrees of expertise, often acting in an untargeted way - perhaps to test their own skills or cause disruption for the sake of it.

Malicious insiders
Use their access to an organisation's data or networks to conduct malicious activity, such as stealing sensitive information to share with competitors.

Honest Mistakes
Sometimes staff, with the best intentions just make a mistake, for example by emailing something sensitive to the wrong email address.

School pupils
Some students simply enjoy the challenge of putting their cyber skills to the test.

3. **Powerful Passwords**

When implemented correctly, passwords are a free, easy and effective way of helping to prevent unauthorised users accessing devices or networks. How to use passwords well:

- Have a different password for each account / service. If this is not possible then make sure your most sensitive accounts (e.g. access to student records) have a unique password.
- If you must write down your passwords, store them securely and away from your device.
- Consider using a password manager – or ask your IT Lead whether this is an option.
- Use two factor authentication (2FA) on sensitive accounts where available. This gives a way of double-checking you really are who you are claiming to be.
- Always lock your account when you step away or stop using your device, even if it's just for a minute. This applies in school or when working from home.

A good way of creating a strong and memorable password is to use three random words. The NSCS website offers more guidance on how to create solid passwords and why three random words might be useful: Three random words or #thinkrandom - NCSC.GOV.UK

Passwords should be easy for you to remember but hard for somebody else to guess. It is recommended that you do not include the following:

- Partner's name
- Child's name
- Pet's name
- Place of birth
- Favourite holiday
- Something related to your favourite sports team
- A list of numbers (e.g. 123456) or words like 'password' or 'qwerty'.

4. **Phishing Attack**

In a typical phishing attack, scammers send fake emails to thousands of people asking for sensitive information (such as bank details) or containing links to bad websites. They do this to steal your details to sell or perhaps to access your organisation's information. All members of staff can play a part in reducing the negative impact of phishing following these guidelines:

- 'If in doubt, call it out'. Always ask for advice if you're not sure if the link or email is legitimate.
- Don't feel silly if you think you have been caught out: it happens to all of us from time to time. But do report this to your Headteacher or IT team as soon as it happens so they can minimise any damage.

Some phishing emails are more sophisticated than others, but it helps to be aware of some of the more obvious clues.

Phishing flags

- Does it contain poor quality images of logos?
- Are there spelling or grammatical errors?
- Does it address you as 'dear friend' rather than by name?
- Is it asking you to act urgently?
- Does it refer to a previous message you don't remember seeing?

5. **Working from home**

You are still responsible for keeping work information safe when you are accessing it at home. These tips can help to minimise the chances of any cyber security incident transferring from home devices to the school network or vice versa.

- Use up-to-date anti-virus software on your own devices.
- Download all software updates as soon as they are offered.
- Ensure all your devices have passcodes. (Even if you only use your laptop for work, for example, this may be synched to your phone or tablet).
- Change any default passwords on devices or software – including your home Wi-Fi.
- Switch on two-factor authentication (2FA) if available for sensitive accounts.

6. **Cyber Security Commandments**

Simple steps can make the world of difference:

- Never ignore software updates – they contain patches that keep you and your school secure
- Always lock your device when you are not using it
- Only download apps and software from official app stores like Google Play or Apple's App Store
- Do not share accounts with others
- Do not be afraid to challenge policies or processes that make your job difficult. Security that gets in the way of doing your work does not work
- Create a culture of questioning – if it looks strange, get a second opinion.