Online Safety Policy

Northwick Park MAT

William Read Primary	Northwick Park Primary and Nursery	Leigh Beck Infant and Nursery
	We Take Pride	…working together

Approved by: Trust Directors Date: 18th May 2023

Last Reviewed: May 2023 Next Review Date: May 2025

Introduction

Key people involved in policy making

Northwick Park Academy Trust	Designated Safeguarding Lead (DSL) team	Emma Lane Lynne Keys, Tracy Smith, Tracy Gravely
	Online-safety lead (if different)	Tracy Smith, Elaine Rising, Sharon Rosher.
	Online-safety / safeguarding link governor	Chair of Governors for each School in the Trust
	PSHE/RSHE lead inc. Mental Health and well being	Kerry John Annette Hyde / Leanne Cooper Polly Wicks / Amy Verkley
	Network manager / other technical support	Elaine Rising and Sharon Rosher Ed Moncur (external)

What is this policy?

Online safety is an integral part of safeguarding and requires a whole Trust, Trust based, cross- curricular approach and collaboration between key Trust leads. Accordingly, this policy is written in line with ‘Keeping Children Safe in Education’ 2019 (KCSIE), ‘Teaching Online Safety in Trusts’ 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing. It also takes into consideration the importance of all stakeholders’ mental health and well-being and the impact these issues can have on this. It is designed to sit alongside The Trust’s statutory Safeguarding Policy. Any issues and concerns with online safety must follow the Trust’s safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the Trust, local area and from the Department for Education. Although many aspects will be informed by legislation and regulations, we involve staff, governors, pupils and parents in writing and reviewing the policy as KCSIE stresses making use of teachers’ day-to- day experience on the ground. This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Acceptable Use Policies (see appendices) for different stakeholders help with this and we ensure that these are reviewed alongside this overarching policy. Any changes to this policy should be immediately disseminated to all the above stakeholders.

Who is in charge of online safety?

Our Online-safety lead for the Trust is also our Deputy Safeguarding lead as KCSIE makes clear that “the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety).” This person is supported in each Trust by a team for online safety, for day to day event and issues. These people liaise with the designated safeguarding lead for the trust and the deputies in all Trust buildings.

What are the main online safety risks today?

Online-safety risks are traditionally categorised as one of the 4 Cs: Content, Contact, Conduct and Commerce. These areas remain a helpful way to understand the risks and potential Trust response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all four.

It has been identified that there is an increase in distress caused by, and risk from, content. For many years, online-safety messages have focussed on 'stranger danger', i.e. meeting strangers online and then meeting them face to face (contact). Whilst these dangers have not gone away and remain important, violent or sexual content is now prevalent – sending or receiving, voluntarily or coerced. Examples of this are the sharing of violent and sexual videos, self-harm materials, and coerced nudity via live streaming. Contact and conduct of course also remain important challenges to address.

How will this policy be communicated?

This policy can only impact upon practice if it is a regularly updated, living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the Trust website
- Available on the internal staff network/drive
- Available in paper format in the staffroom and from the individual school offices
- Part of Trust induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which are in an accessible language appropriate to these groups).
- AUPs issued to whole Trust community, on entry to the Trust, with annual reminders of where to find them if unchanged, and reissued if updated after annual review
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement.

Contents

Overview

Aims

This policy aims to:

- Set out expectations for all Northwick Park Academy Trust's 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 Trust gates and Trust 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 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, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the Trust, supporting the Trust ethos, aims and objectives, and protecting the reputation of the Trust and profession
- Establish clear structures by which online misdemeanors will be treated, and procedures to follow where there are doubts or concerns (with reference to other Trust policies such as Behaviour Policy or Anti-Bullying Policy)

Further Help and Support

Our internal Trust channels are always followed first for reporting and support, as documented in Trust policy documents, especially in response to incidents which are reported in line with our Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and normally the head teacher will handle referrals to the LA designated officer (LADO). The local authority, academy trust or third-party support organisations we work with also have advisors to offer general support.

Beyond this, there are external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Whistleblowing Helpline, as well as hotlines for hate crime, terrorism and fraud which are shared with parents, and anonymous support for children and young people.

Scope

This policy applies to all members of the Northwick Park Academy Trust community (including staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their Trust role.

Roles and responsibilities

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

Executive Headteacher/Trust CEO – Mrs Emma Lane

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-Trust safeguarding
- That members of SLT oversee activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- 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 Partnerships
- Liaise with the Online Safety Leads on all online-safety issues which might arise and receive regular updates on Trust issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the Trust's provision follows best practice in information handling; work with the DPO, DSL and 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 the Trust implements and makes effective use of appropriate ICT systems and services including Trust-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 suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- 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 governors are regularly updated on the nature and effectiveness of the Trust's arrangements for online safety
- Ensure the Trust website meets statutory requirements (see appendices for website audit document)

Designated Safeguarding Lead / Online Safety Lead – DSL – Emma Lane / OSL Tracy Smith

Keeping Children Safe in Education states that:

"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)." They *"are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college"*

They *"*can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety Lead

The Online Safety Lead will:

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), (where these roles are not combined)
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with staff to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with (school/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant)

- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce
- Facilitate training and advice for all staff:
    - all staff have read KCSIE Part 1 and all those working with children Annex A
    - it would also be advisable for all staff to be aware of Annex C (online safety)
    - cascade knowledge of risks and opportunities throughout the organisation

Governing Body, led by Online Safety / Safeguarding Link Governor – Individual Schools Chair of Governors

The DfE guidance "Keeping Children Safe in Education" states:

> "Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"
> "Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".
This review will be carried out by the Chair of Governors in each individual schools and a Director of the Trust to oversees for the Trust. whose members will receive regular information about online safety incidents and monitoring reports. The Chair of the governing body will take on the role of Online Safety Governor to include:

- **regular meetings with the Designated Safeguarding Lead / Online Safety Lead**
- **regularly receiving (collated and anonymised) reports of online safety incidents**
- **checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)**
- **Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually.** (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- **reporting to relevant *governors group/meeting***
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

All staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up

- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are in the school building that they are working in across the Trust
- Read 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).
- Read and follow this policy in conjunction with the Trust's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with Trust procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and code of conduct/handbook
- Notify the DSL/OSL if policy does not reflect practice in your school building and follow escalation procedures if concerns are not promptly acted upon e.g. via self-referring to Social Care or LADO
- Identify opportunities to thread online safety through all Trust 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, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask the OSL what appropriate filtering and monitoring policies are in place)
- To 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
- Prepare and check all online source and resources fully before using within the classroom, including adverts that may be present in video clips etc.
- Encourage pupils/students to follow their acceptable use policy, remind them about it and enforce Trust sanctions
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be 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 – let the DSL/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety issues.
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the Trust hours and site, and on social media, in all aspects upholding the reputation of the Trust and of the professional reputation of all staff. More guidance on this point can be found in this Online Reputation guidance for Trusts.

PSHE / RSHE Lead/s – Leanne Cooper / Kerry John/Annette Hyde

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Ensure that all staff dealing with Online Safety issues consider the implications that these issues may have in impacting the mental health and well-being of all of the children and staff involved.

Computing Lead – Tracy Smith

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Work closely with all members of the ICT team to ensure curriculum coverage and support for all staff in dealing with issues and SLT.
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in Trust to ensure a common and consistent approach, in line with acceptable-use agreements

Subject leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and pupils alike
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Trusts can be applied in your context
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues,

approaches and messaging within Computing
- Ensure subject specific action plans also have an online-safety element

Network Manager/technician – Elaine Rising / Sharon Rosher

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Keep up to date with the Trust's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / data protection officer to ensure that Trust systems and networks reflect Trust policy
- Ensure 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
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team
- Maintain up-to-date documentation of the Trust's online security and technical procedures
- To report online-safety related issues that come to their attention in line with Trust policy
- 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, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Monitor the use of Trust technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with Trust policy
- Work with the Head teacher to ensure the Trust website meets statutory DfE requirements

IT Provider

The DfE Filtering and Monitoring Standards says:

"Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."

"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."

"The IT service provider should have technical responsibility for:

- *maintaining filtering and monitoring systems*
- *providing filtering and monitoring reports*
- *completing actions following concerns or checks to systems"*
- *identify risk*
- *carry out reviews*
- *carry out checks"*

In all Trust schools we use a technology service provided by an outside contractor, and it is the responsibility of the school technology teams to ensure that the provider carries out all the online safety measures that are our obligation and responsibility.

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to (insert relevant person) for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- *monitoring systems are implemented and regularly updated as agreed in school policies*

Data Protection Officer (DPO) – Tracy Smith (Trust) Lauri Almond (Judicium)

Key responsibilities:

- Be aware that 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 Trusts’ (August 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. Lawful and secure information sharing between Trusts, Children’s Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced ‘safeguarding’ as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in Trusts are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant 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.”

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)’. However, some local authorities require record retention until 25 for <u>all</u> pupil records.

- Work with the DSL, headteacher and governors 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

Volunteers and contractors

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the Trust's acceptable use policies cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/carers

Key responsibilities:

- Read, sign and promote the Trust's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible 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 the Trust staff, volunteers, governors, contractors, pupils or other parents/carers.

Education and curriculum

The following subjects have the clearest online safety links:

- PSHE
- Relationships education, relationships and sex education (RSE) and health
- Computing
- Citizenship
- Mental Health and Well-being

However, as stated in the role descriptors above, it is the role of all staff to identify 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, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended Trust 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 Northwick Park Academy Trust, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World' from UKCIS (the UK Council for Internet Safety).

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Handling online-safety concerns and incidents

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

> *"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:*
>
> - *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"*

It is vital that all staff recognise that online-safety is a part of safeguarding as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship.

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

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures, this may include
    - Non-consensual images

  - Self-generated images
  - Terrorism/extremism
  - Hate crime/ Abuse
  - Fraud and extortion
  - Harassment/stalking
  - Child Sexual Abuse Material (CSAM)
  - Child Sexual Exploitation Grooming
  - Extreme Pornography
  - Sale of illegal materials/substances
  - Cyber or hacking offences under the Computer Misuse Act
  - Copyright theft or piracy

Trust procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including Trust sanctions)
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

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

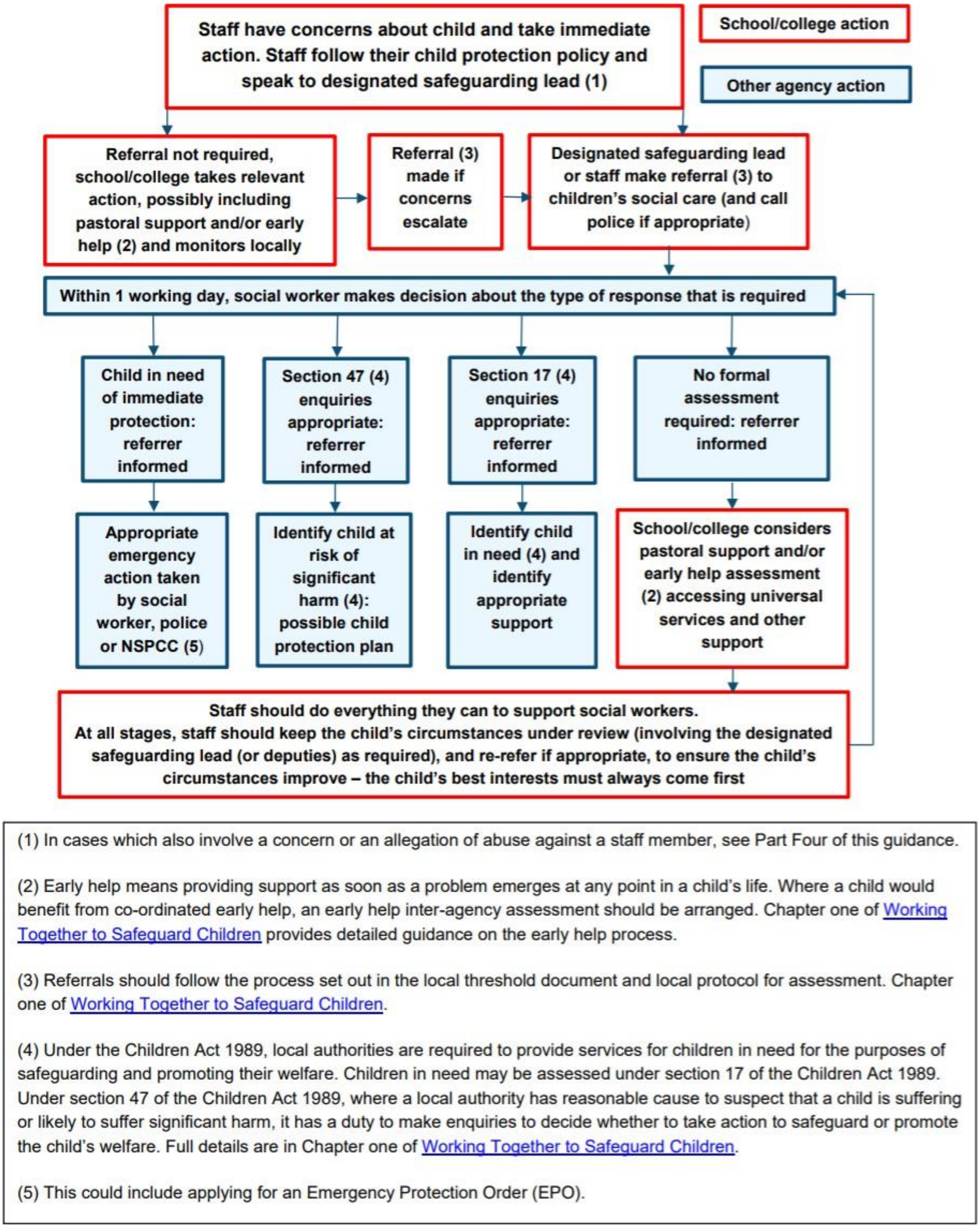
Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

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

The Trust will actively seek support from other agencies as needed (i.e. the local authority, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

Actions where there are concerns about a child

The following flow chart (it cannot be edited) is taken from page 13 of Keeping Children Safe in Education 2019 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead (1)

School/college action

Other agency action

Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help (2) and monitors locally

Referral (3) made if concerns escalate

Designated safeguarding lead or staff make referral (3) to children's social care (and call police if appropriate)

Within 1 working day, social worker makes decision about the type of response that is required

Child in need of immediate protection: referrer informed

Section 47 (4) enquiries appropriate: referrer informed

Section 17 (4) enquiries appropriate: referrer informed

No formal assessment required: referrer informed

Appropriate emergency action taken by social worker, police or NSPCC (5)

Identify child at risk of significant harm (4): possible child protection plan

Identify child in need (4) and identify appropriate support

School/college considers pastoral support and/or early help assessment (2) accessing universal services and other support

Staff should do everything they can to support social workers.
At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

(1) In cases which also involve a concern or an allegation of abuse against a staff member, see Part Four of this guidance.

(2) Early help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Chapter one of Working Together to Safeguard Children provides detailed guidance on the early help process.

(3) Referrals should follow the process set out in the local threshold document and local protocol for assessment. Chapter one of Working Together to Safeguard Children.

(4) Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. Children in need may be assessed under section 17 of the Children Act 1989. Under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that a child is suffering or likely to suffer significant harm, it has a duty to make enquiries to decide whether to take action to safeguard or promote the child's welfare. Full details are in Chapter one of Working Together to Safeguard Children.

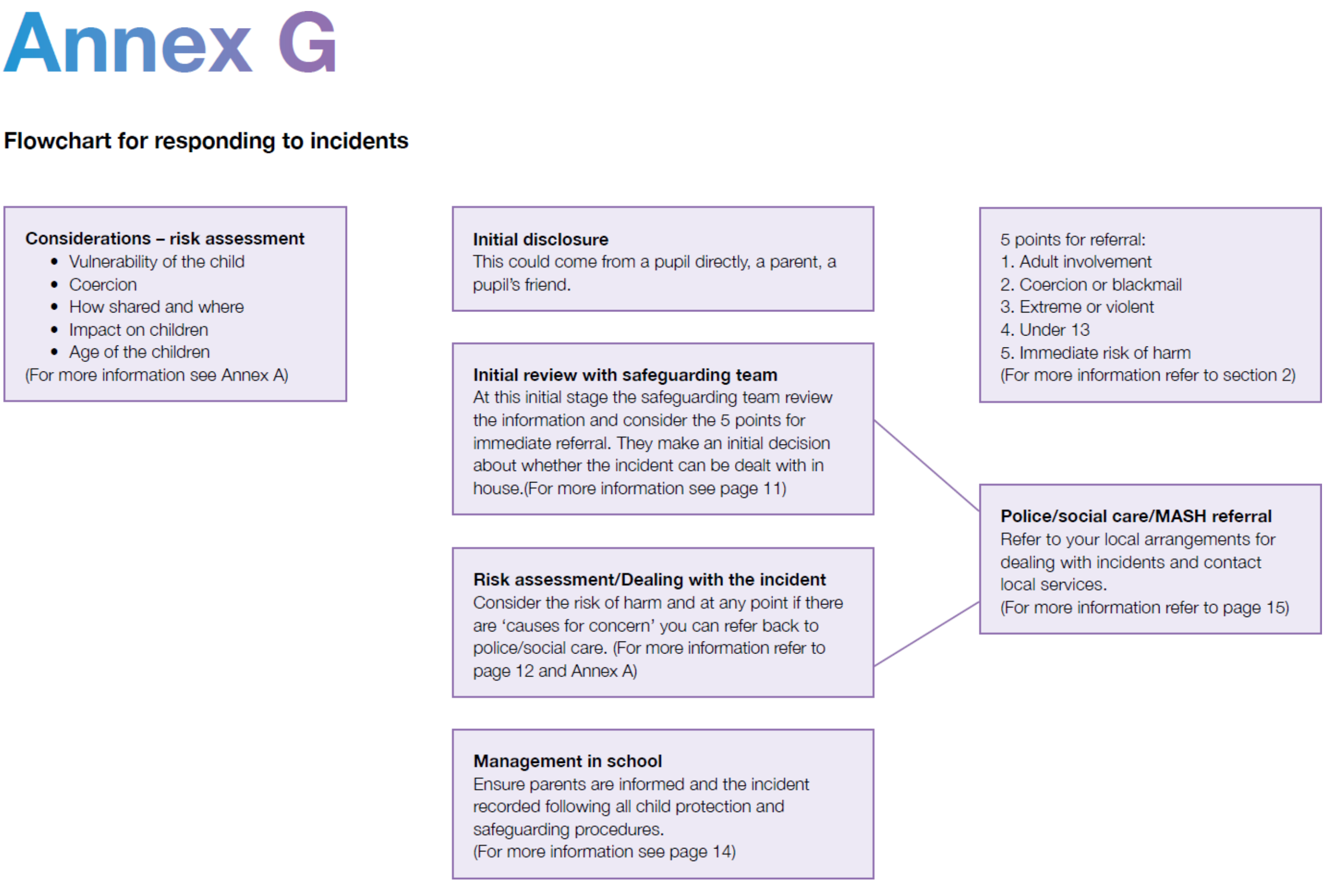
(5) This could include applying for an Emergency Protection Order (EPO).

Sexting

All Trusts (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

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

The Trust DSL will in turn use the full guidance document, Sexting in Trusts and Colleges to decide next steps and whether other agencies need to be involved.



Annex G

Flowchart for responding to incidents

Considerations – risk assessment
- Vulnerability of the child
- Coercion
- How shared and where
- Impact on children
- Age of the children

(For more information see Annex A)

Initial disclosure
This could come from a pupil directly, a parent, a pupil's friend.

Initial review with safeguarding team
At this initial stage the safeguarding team review the information and consider the 5 points for immediate referral. They make an initial decision about whether the incident can be dealt with in house.(For more information see page 11)

Risk assessment/Dealing with the incident
Consider the risk of harm and at any point if there are 'causes for concern' you can refer back to police/social care. (For more information refer to page 12 and Annex A)

Management in school
Ensure parents are informed and the incident recorded following all child protection and safeguarding procedures.
(For more information see page 14)

5 points for referral:
1. Adult involvement
2. Coercion or blackmail
3. Extreme or violent
4. Under 13
5. Immediate risk of harm

(For more information refer to section 2)

Police/social care/MASH referral
Refer to your local arrangements for dealing with incidents and contact local services.
(For more information refer to page 15)

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying should be treated like any other form of bullying and the Trust bullying policy should be followed for online bullying, which may also be referred to as cyberbullying.

Northwick Park Academy Trust's has a separate online bullying policy linked to the anti-bullying policy. This can be found in the Appendices to this policy

Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right. It would be useful for all staff to be aware of this guidance: paragraphs 45-49 cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

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

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

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

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

Where pupils contravene these rules, the Trust behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook and infringements policy (see appendix)

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

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Northwick Park Academy Trust community. These are also governed by Trust Acceptable Use Policies and the Trust social media policy.

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

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the Trust community, Northwick Park Academy Trust will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the Trust 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.

Data protection and data security

There are 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 Trusts' (August 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff – note the red and purple highlights:

"**GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe.** Lawful and secure information sharing between Trusts, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4). When Designated Safeguarding Leads in Trusts are considering whether, or not, to share safeguarding information (especially with other agencies) **it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant 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**."

All pupils, staff, governors, volunteers, contractors and parents are bound by the Trust's data protection policy and agreements.

Rigorous controls on the LGfL network, USO sign-on for technical services, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection: Sophos Anti-Virus, Sophos Anti-Phish, Malware Bytes, Egress.

The head teacher, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of Egress to encrypt all non-internal emails is compulsory for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

Appropriate filtering and monitoring

The DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education" states:

"It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified…
The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards…"

The school filtering and monitoring provision is provided by LGFL as part of their Broadband contract, and is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced**.**

Filtering

- The school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes (see Appendix for more details).
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)
- younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle
- the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the LGFL Report Harmful Content site.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)

- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- *pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.*
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT
- password policy and procedures are implemented. (consistent with guidance from the National Cyber Security Centre)
- the security of their username and password and must not allow other users to access the systems using their log on details.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- all school networks and systems will be protected by secure passwords. Passwords must not be shared with anyone
- the administrator passwords for school systems are kept in a secure place, e.g. school safe.
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- The Technology Team in each school is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider
- systems are in place to control and protect personal data and data is encrypted at rest and in transit. (See school personal data policy template in the appendix for further detail)
- mobile device security and management procedures are in place (where mobile devices are allowed access to school systems). (Schools may wish to add details of the mobile device security procedures that are in use).
- guest users are provided with appropriate access to school systems based on an identified risk profile.

Electronic communications

Please read this section alongside references to pupil-staff communications in the overall Trust Safeguarding Policy, and in conjunction with the Data Protection Policy. This section only covers electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

Email

- Pupils at this Trust use the Office 365 system school emails
- Staff at this Trust use the Office 365 system for all Trust related emails

Both these systems are linked to the USO authentication system and are fully auditable, trackable. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email is the only means of electronic communication to be used between staff. Use of a different platform must be approved in advance by the data-protection officer / head teacher 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 Head teacher (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 DSL/Head teacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email.
  - If data needs to be shared with external agencies Egress systems are available alongside the S2S systems for school to school data transfer e.g. for a transferring pupil.
  - Internally, staff should use the Trust network, including when working from home via Microsoft Cloud
- Pupils, in all year groups, are restricted to emailing within the Trust and cannot email external accounts
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the Trust into disrepute or compromise the professionalism of staff
- Pupils and staff are NOT allowed to use the email system for personal use and 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.

Education and online safety is an important part of every child’s Computing learning journey to ensure that they are fully informed about staying safe and protecting themselves.

- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and more generally (for example personal accounts set-up at home) i.e.
- not to give out their e-mail address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/carer;
- that an e-mail is a form of publishing where the message should be clear, short and concise;
- that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages;
- not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
- not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
- that forwarding 'chain' e-mail letters is not permitted.

Children are also taught the appropriate behaviours to adopt if they receive an inappropriate or offensive email, such as closing it and seeking advice from a teacher or responsible adult, but never replying to it. This will allow the teacher or responsible adult to check the message, talk through the issues, reassure the pupil that it was not their fault that they received such a message, and take any other action as appropriate.
As bullying, abuse or harassment by email is becoming an increasing problem, pupils are made aware of the appropriate actions to take if they receive unwanted or upsetting email messages, and should guard against giving out personal information at all times.

Advice and sanctions for dealing with incidents of this nature can be found in our infringements policy.

See also the social media section of this policy.

Trust websites

The Trust website is a key public-facing information portal for the Trust community (both existing and prospective stakeholders) with a key reputational value. The Head teacher and Governors have delegated the day-to-day responsibility of updating the content of the website to Elaine Rising and Sharon Rosher, under the guidance of members of the Senior Leadership Team. The site is hosted E4Education.

The DfE has determined information which must be available on a Trust website and Sarah Gould and Tracy Smith work within this to ensure that the school website is compliant. It is our policy that our website is inviting, easy to navigate and effective, whilst protecting the safety and integrity of the pupils, staff and school.

In order to ensure that every child in our care is safe, the same principles should apply to the virtual presence of a school as would be applied to its physical buildings. We ensure that no individual child can be identified or contacted either via, or as a result of a visitor using, the school website.

To ensure that our website is appropriate effective and safe:

- The Academy Senior Leadership Team takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;

- Uploading of information is restricted to the ICT Technicians
- The school web site complies with the school's guidelines for publications;
- Most material is our own work, produced in school, but where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address and telephone number. Year Group email addresses are published for children to send home learning tasks to teachers should the school be closed for any reason other than planned closures. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have attached personal details;
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school. This is then compiled and distributed to all members of staff;
- We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
- Staff, parents and pupils sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computing scheme of work;
- Pupils are taught about how images can be abused in their E-Safety education programme.
- We ensure that the site is monitored on a weekly basis by the administration to ensure that the safety and integrity of the children is not compromised.

Where other staff submit information for the website, this goes via a member of SLT and they are asked to remember:

- Trust have the same duty as any person or organisation to respect and uphold copyright law – Trusts have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. There are many open-access libraries of high-quality public-domain images that can be used (e.g. pixabay.com for marketing materials – beware some adult content on this site). Pupils and staff at LGfL Trusts also have access to licences for music, sound effects, art collection images and other at curriculum.lgfl.net
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

Cloud platforms

Many Trusts are recognising the benefits of cloud computing platforms, not just for cost savings but to enhance teaching and learning.

This Trust adheres to the principles of the DfE document 'Cloud computing services: guidance for Trust leaders, Trust staff and governing bodies'.

For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush – never share it with anyone!"), expert administration and training can help to keep staff and pupils safe, and to avoid incidents. The data protection officer and network manager analyse and document systems and procedures before they are implemented, and regularly review them.

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- The DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought
- 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
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only Trust-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Digital images and video

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

- For displays around the Trust
- For the newsletter
- For online prospectus or websites
- For a specific high profile image for display or publication

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.
Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the Trust's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Northwick Park Academy Trust, no member of staff will ever use their personal phone to capture photos or videos of pupils.

Photos are stored on the Trust network in line with the retention schedule of the Trust Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. We do allow parents to take photographs and videos at school events, but are told not to share these on social media. They are informed that if this does occur they will be removed by contacting the provider.

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

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

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

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

Social media

Northwick Park Academy Trust's SM presence

Northwick Park Academy Trust works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the Trust online). Few parents will apply for a Trust place without first 'googling' the Trust, and the Ofsted pre-inspection check includes monitoring what is being said online (Mumsnet is a favourite).
Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve Trusts' (and staff members') online reputation.

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

Tracy Smith (LB) and Lynne Keys (NP) are responsible for managing our individual school Facebook accounts and checking our Wikipedia and Google reviews. They follow the guidance in the Safer Internet Centre online-reputation management document

Staff, pupils' and parents' SM presence

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

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

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

Many social media platforms have a minimum age of 13, but the individuals within the Trust regularly deal with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

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

Parents can best support this by talking to their children about the apps, sites and games they use, with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at Trust the next day). You may wish to introduce the Children's Commission Digital 5 A Day (see appendix 8).
It is encouraging that 73% of pupils trust their parents on online safety (although only half talk about it with them more than once a year at the moment).

Each school in the Trust has an official Facebook account (managed by Tracy Smith and Lynne Keys) and will respond to general enquiries about the Trust, but asks parents/carers not to use these channels to communicate about their children.

Email is the official electronic communication channel between parents and the Trust, and between staff and pupils.

Pupils/students are not allowed to be 'friends'* with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

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

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

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

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

Trust into disrepute. Members of staff are also reminded that photographs which they post themselves or are tagged in may cause them to been seen in a less positive light.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there have been 200 Prohibition Orders issued to teachers over the past four years related to the misuse of technology/social media.

All members of the Trust community are reminded that particularly in the context of social media, it is important to comply with the Trust policy on Digital Images and Video and permission is sought before uploading photographs, videos or any other information about other people.

Monitoring of public Social Media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- the school should effectively respond to social media comments made by others according to a defined policy or process.
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

Device usage

Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

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

- **Pupils/students** in upper Key Stage 2 are allowed to bring mobile phones in for emergency use only. During lessons, phones must remain turned off at all times and be handed into the school office at the start of the day. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to the phone being taken away for the rest of the day and the withdrawal of mobile privileges. Important messages and phone calls to or from parents can be made at the Trust office, which will also pass on messages from parents to pupils in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during Trust hours. See also the Digital images and video section and Data protection and data security section. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may granted permission to do so by the Head teacher or a member of SLT.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos.

If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the head teacher or a member of SLT should be sought and this should be done in the presence of a member staff.

- **Parents** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at Trust events, please refer to the Digital images and video section of this document. Parents are asked not to call pupils on their mobile phones during the Trust day; urgent messages can be passed via the Trust office.

Network / internet access on Trust devices

- **Pupils/students** are not allowed networked file access via personal devices. However, they are allowed to access the school wireless internet for school-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during Trust hours. See also the Digital images and video section and Data protection and data security section. Child/staff data should never be downloaded onto a private phone.
- **Volunteers, contractors, governors** have no access to the Trust network or wireless internet on personal devices, subject to the acceptable use policy. All internet traffic is monitored.
- **Parents** have no access to the Trust network or wireless internet on personal devices. All internet traffic is monitored.

Trips / events away from Trust

For Trust trips, teachers will be able to use personal mobile phones for any authorised or emergency communications with the head teacher or the school office in order to contact pupils and parents. Any deviation from this policy will be notified immediately to the head teacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher’s private phone number

Searching and confiscation

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

Appendices

1. Online Bullying Policy
2. *Acceptable Use Policies (AUPs) for:
    - *Pupils KS1 & KS2
    - *Staff, Volunteers Governors & Contractors
    - *Parents
3. Infringements Policy
4. Mobile Phone Policy
5. Social Media Policy
6. Online Reputation Guidelines
7. Digital 5-a-day
8. E-Security Policy
9. Online-Safety Questions from the Governing Board (UKCIS)
10. Legislation
11. Links to other organisations

Northwick Park Academy Trust

Safeguarding Policy

At Northwick Park Academy Trust the safety and protection of the children in our care is paramount.

Section 175 of the 2002 Education Act and Section 11 of the 2004 Children Act places upon all those who work with children a duty to safeguard and promote their welfare by creating a safe learning environment and where there are child welfare concerns, taking swift action to address them.

This statement is held true in every area of the curriculum including Computing.

Although the use of ICT and the internet provide ever increasing opportunities for children to expand their knowledge and skills, it is also the case that the use of such technology may sometimes expose children to the risk of harm. Apart from the risk of children accessing internet sites which contain unsuitable material, risks to the well being of children may also exist in a variety of other ways.

It is known that adults who wish to abuse may pose as children to engage and then meet up with the children or young people they have been in communication with. This process is known as 'Grooming' whereby an adult prepares a child or young person to be abused. The process may take place over a period of months using chat rooms, social networking sites and mobile phones. An adult may pretend to be a peer and gradually convince the child or young person that they are their boyfriend or girlfriend, establishing a relationship of apparent trust with the intended victim and making it difficult for the child to then speak out. Increasingly bullying is conducted on the internet or by the use of text messages and is therefore harder for schools to notice and deal with.

At Northwick Park Academy Trust it is our high priority to create a safe learning environment through having effective arrangements in place to address a range of issues and ensure that our policies and procedures in place are reviewed annually and adhered to by all staff, teaching and non teaching whether in a paid or voluntary capacity.

These issues are also covered and incorporated into our Online Safety, Behaviour, Acceptable Use and Child Protection Policies.

It is vital that all staff are aware of the signs which might indicate that a child is being groomed, bullied or being subjected to inappropriate material and know how to take steps to begin to address this and safeguard and support the child. All staff are aware of these matters and are actively involved in the creation and implementation of the guidelines for safeguarding children.

At Northwick Park Academy Trust we strive to create a 'No Blame' culture and we encourage our children to be confident that this culture is evident so that when it comes to reporting inappropriate incidents involving the internet or mobile technology they are able to do this without fear. As part of this staff are informed and updated because as with all forms of harm or abuse, there is no exhaustive list of signs or indicators to watch out for. But these can include: changes in children's behaviour, demeanour, physical appearance and presentation, language or progress. Also we are vigilant that all staff know who to go to if they have a concern that a child or young person might be at risk or suffering harm as a result of the use of these technologies.

Northwick Park Academy Trust

Online Bullying Policy

At Northwick Park Academy Trust we know that it is important to acknowledge the unfortunate misuses of technology. At Northwick Park Academy Trust we recognise the existence of online bullying and the severity of the issue.
Bullying is based on unequal power relations, real or perceived. It will usually be repeated and be difficult to defend against. It is intended to hurt the recipient emotionally and/or physically. It can manifest verbally, in writing or images, and can be done physically, financially (including damage to property) or through social isolation. Verbal bullying is the most common form especially within schools.

At Northwick Park Academy Trust we fully recognise that bullying can also be done through the use of communication technology.

Online bullying is bullying through the use of communication technology like mobile phone text messages, e-mails or websites. This can take many forms for example:

- Sending threatening or abusive text messages or e-mails, personally or anonymously.
- Making insulting comments about someone on a website, social networking site (e.g.: Twitter or Facebook) or online diary (blog).
- Making or sharing derogatory or embarrassing videos of someone via mobile phone or e-mail.

At Northwick Park Academy Trust online bullying issues are dealt with in and appropriate way in relation to the severity and frequency of the issue.

Appropriate actions if an online bullying incident occurs -

- Advise the child not to respond to the message
- Refer to relevant policies including online safety, acceptable use, anti-bullying and PHSE and apply appropriate sanctions
- Secure and preserve any evidence
- Inform the sender’s e-mail service provider
- Inform Head teacher and Senior Management team,
- Notify parents of the children involved
- Consider delivering a parent workshop for the school community
- Consider informing the police depending on the severity or repetitious nature of offence

If malicious or threatening comments are posted on an Internet site about a pupil or member of staff.

- Inform site and request the comments be removed if the site is administered externally
- Secure and preserve any evidence
- Inform Head teacher and Senior Management team
- Inform parents
- Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html
- Endeavour to trace the origin and inform police as appropriate

Reporting incidents

At Northwick Park Academy Trust any issues of online bulling which may arise will be dealt with the same as any other bullying issue in line with the proposed chain of reporting (outlined above) and all of our children and staff are made aware of this. To enable this to happen we encourage our children to be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

Online bullying Education

As part of our on-going efforts to educate our children about the dangers and effects of online bullying and how to recognise this every child takes part in a series of lessons focussing on e-safety as well as this being built into every lesson which involves ICT. These lessons form a part of our Computing curriculum and are adapted from the Education of a connected world document. This teaching includes sharing messages from 'Think u know', 'Hector's World' and the SMART rules for internet safety

We also share these points for safe practice by displaying them and the SMART rules within all ICT areas, corridors and classrooms –

Keep personal information private
This includes details such as name, address, photos of yourself and your friends, email addresses, home and mobile phone numbers, school name, membership of clubs, information on family and friends, and passwords.
Don't believe everything you read
Just because someone online tells you that they are 15 doesn't mean they are telling the truth.
Use netiquette
Be polite to others online as you would offline. If someone treats you rudely, or is mean, you should not respond. If the abusive messages continue, seek help from a teacher, parent or carer.
Protect yourself
Never arrange to meet someone you have met online.
Never send messages when angry
Wait until you have calmed down and had time to think. Once you've sent a message in anger, it's extremely difficult to undo the damage that can be done.
Never open a message from someone you don't know
Delete strange emails or text messages from people you don't know. If in doubt, seek advice from a teacher, parent or carer.
If it doesn't look or feel right, it probably isn't
If you ever see anything on the internet, or receive an email or text message that makes you feel uncomfortable, switch off the computer or phone and seek advice from a teacher, parent or carer.
You don't have to be 'always on' – turn off, disconnect, unplug
Give yourself a break. Don't stay online for too long.
Don't reply to messages from online bullies
Even though you may really want to, this is exactly what online bullies want.
Don't keep bullying to yourself
You are not alone! Tell an adult you know and trust. They can help you combat the online bullying.

These issues are also addressed as part of the school's PSHE curriculum, Health week and shared in assemblies.

Working with Parents

To support the dealing with the issues around online bullying in the wider school community parents are provided with information leaflets including Young Children and Social Networking Sites from Childnet International. Parents are invited to share and discuss and issues with the class teachers, Online Safety co-ordinator Tracy Smith (LB), Elaine Rising (NP) or Sharon Rosher (LB)and the Head Teacher to resolve any issues.

Northwick Park Academy Trust

Acceptable Use Policy

At Northwick Park Academy Trust we recognise the importance of ICT in education and the needs of pupils to access the facilities available with the school.

Aims

The aims of this Acceptable Use Policy are to:

- Ensure that pupils benefit from all learning opportunities offered by the internet resources provided by the school in a safe and controlled manner.
- Ensure that all staff benefit from internet access, with clear guidance on safe and acceptable use.
- Make staff and pupils aware that Internet use in school is a resource and a privilege. If the terms are not met then the privilege will be taken away.
- Provide guidance to staff and pupils about the acceptable use of mobile technologies, both the school's and personal items that are brought into school.

Expectations

- It is expected that all users of the network and internet including staff, pupils, parents and visitors will follow the conditions of this policy.
- A responsible approach to resources should be shown at all times.
- All activity should be appropriate to staff CPD or pupils' education.
- Access should only be made via the authorised account and password, which should not be made available to any other person.
- Access is a privilege not a right and users need to demonstrate a responsible attitude and behaviour.
- All users should show consideration for other uses both locally and with whom they may come into contact on the Internet.

Use of the Network, the Internet and facilities such as the e-mail are intended for educational purposes only. Any communication should be honest, legal, decent and true. It must be recognised that any view communicated may be deemed to be the view of the school, governing body and in some circumstances that of the LA.

At Northwick Park Academy Trust our computer system is owned and maintained by the school and contracted services. The computer system refers to all computers and associated equipment belonging to the school, whether part of the school's integrated network or stand-alone, or taken offsite.

Professional use of the computer system is characterised by activities that provide children with appropriate learning experiences; or allow adults to enhance their own professional development. The school recognises that technologies such as the Internet and e-mail will have a profound effect on children's education and staff professional development in the coming years and the school's Internet Access Policy has been drawn up accordingly.

Internet access within school

The purpose of internet access is to raise educational standards, support professional development and enhance the school's management, information and business administration systems.

Teachers and pupils will have opportunities to access educational materials and good curriculum practice, be able to communicate with the advisory and support services, professional associations and colleagues, exchange curriculum and administration data with the LA and DfE, receive up-to-date information and participate in government initiatives such as the Essex Grid for Learning and the Virtual Teacher centre.

To cover all points of internet usage we have developed an internet policy which parents are informed of by letter and is available to read by parents and others on request.

At Northwick Park Academy Trust we are aware that some material found on the internet will be unsuitable for children. The school will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate materials on the internet.
The following key measures have been adopted to combat this possibility –

- Our internet access has a supplier and school defined filtering system

- Children will access the internet within classrooms, the Creative suite and the computer suites, under constant supervision.

- Staff will pre-select sites before using them to ensure they are age appropriate and suitable.

- Our Internet Rules are clearly displayed in all computer suites

- The Computing subject leader and the System Administrator will regularly check random files and folders to check they comply with this policy.

If there is an incident in which a pupil is exposed to something inappropriate the school will respond to the situation quickly and on a number of levels. Responsibility for handling incidents involving the children is taken by the ICT subject leader and the Child Protection Officer and the pupil's class teacher. All teaching staff will be made aware of the incident at a staff meeting if appropriate. If one or more pupils discover inappropriate material the first priority will be give to the support of the children. The parents/carers will be informed and given an explanation of the course of action the school has taken. If staff or pupils discover unsuitable sites the ICT subject leader will be informed. This website will then be reported to the internet provider and the LA. If it is thought that the material is illegal it maybe that the site will need to be referred to CEOP and the police.

Access to the internet is a planned part of the curriculum that enriches and extends learning activities and is integrated into all schemes of work, with a clear objective.

Different ways of accessing information from the internet are used depending upon the age of the pupils and the nature of the materials.

- Access to the internet maybe by the teacher for demonstrations purposes pupils may access teacher prepared resources
- Pupils may be directed to a specific web address saved within their favourites.
- Pupils will be expected to observe our internet rules and will be made aware that checks can and will be made at random of stored files and accessed sites.

- Pupils will be educated in taking responsibility for their own internet access via the E-safety teaching in each year group.

Pupils will also be taught that the information that they may find on the internet needs to be evaluated for truth, bias, and relevance before being used. Children will also be taught about copyright and the usage of materials they may find.

E-mail use

As part of the ICT curriculum children are taught how to send and receive e-mails and e-mail conventions. It is actively encouraged that staff and pupils will only use an agreed e-mail address within the school for school related business.
All of the issues regarding e-mail us and safety are set out within our online safety policy.

School website and Home/School Links

We as a school, wish that our web site reflects the diversity of activities, individuals and education that can be found at Northwick Park Academy Trust. However, the school recognises the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when we consider material for publication on the Internet, the following principles are borne in mind:

- No video recording may be published without the written consent of the parents/legal guardian of the child concerned, and the child's own verbal consent;

- Surnames of children are not published, especially in conjunction with photographic or video material;

- No link should be made between an individual and any home address (including street names);

- Where the person publishing material suspects that there may be child protection issues at stake then serious consideration must be taken as to whether that material should be published or not. In the case of a simple piece of artwork or writing, this may well be fine, but images of that child should not be published. If in any doubt at all, refer to the person responsible for child protection.

For further information please refer to the Safe School website Policy.

Unacceptable use

At Northwick Park Academy Trust unacceptable usage of the internet will not be tolerated. The following activities, whilst not exhaustive, are seen as unacceptable:-

- The access to or creation, transmission or publication of any offensive, obscene language or indecent images, sounds, data or other material.

- The creation, transmission or publication of any data capable of being displayed or converted to materials which will offend, endanger or bring the school into disrepute.

- The creation, transmission or publication of any materials that may cause offence, inconvenience or cause needless anxiety.

- The creation, transmission or publication of defamatory material.

- The receipt or transmission of materials that infringes copyright or the conditions of the Data Protection Act 1984.

- Use for personal financial gain, gambling, political purposes or advertising is forbidden.

- Corrupting or destroying other user's data, violating the privacy of other users or disrupting the work of any other users is also unacceptable.

Through our Cache system and the E_2BN filtering systems in place at our school, all Internet activity is monitored by the system. It is the responsibility of the Computing subject leader and system administrator to review this activity periodically. It is the duty of these people to report any transgressions of the school's Internet policy, acceptable use policy, or examples of bullying or intimidation detected by the system to the Head teacher. Occasionally, it may be necessary for the ICT subject leader to investigate attempted access to blocked sites, and in order to do this, the ICT subject leader and system administrator's Internet access rights are set to "Unrestricted". Whenever this happens, this should be recorded in the ICT violations register, and the Head teacher notified.

All serious transgressions of the school's Internet Access Policy are recorded in the school's ICT violations register. The violations register can be found in the main ICT suite.

Transgressions of Internet Policy and use of inappropriate language can be dealt with in a range of ways, including removal of Internet access rights; computer system access rights; meetings with parents or even exclusion; in accordance with the severity of the offence and the school's Behaviour Policy.

Breaches of Internet Access Policy by staff will be reported to the Head teacher and will be dealt with according to the school's and LEA's disciplinary policy, or through prosecution by law.

All of these infringements and their consequences are set out in our Infringements Policy.

Use of portable equipment

The school provides portable ICT equipment such as laptop computers, Ipads, colour printers and digital cameras to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities.

The acceptable use of this equipment is the same as those set out in this and the individual policies.

- Equipment may be in the care of a specific individual, but it is expected that all staff may wish to benefit from the use of a laptop computer and access should be negotiated with the individual concerned. Any difficulties should be referred to the ICT Subject leader.

- Certain equipment will remain in the care of the ICT subject leader or system administrator, and may be booked out for use according to staff requirements. Once equipment has been used, it should be returned to the resource area.

- Equipment such as laptop computers are encouraged to be taken offsite for use by staff in accordance with the Acceptable Use Statement and Internet Access Policy and that the equipment is fully insured from the moment it leaves the school premises. Note: our school insurance policy provides cover for equipment taken offsite, provided it is looked after with due care, i.e. not left in view on a car seat etc.

- Any costs generated by the user at home, such as phone bills, printer cartridge etc. are the responsibility of the user.

- Where a member of staff is likely to be away from school through illness, professional development (such as secondment etc.) or maternity leave, arrangements must be made for any portable equipment in their care to be returned for school. In the event of illness, it is up to the school to collect the equipment if the individual is unable to return it.

- If an individual leaves the employment of the school, any equipment must be returned.

- No other software, whether licensed or not, may be installed on laptops in the care of teachers as the school does not own or control the licences for such software.

Responsibilities of making the policy effective.

In order to ensure that this policy is fully effective all staff have had access to it and this will continue.

- The class teacher ensures that all pupils in the class are aware of the rules of use.
- All staff ensure they are familiar with the rules and conditions of all of the policies related to Computing.
- We inform parents and carers of the policy and rules.
- We obtain parent/carer’s permission for internet use according to the rules.
- Staff guide children in their use of the Internet towards appropriate materials.
- We display appropriately worded versions of the rule for using the computers in the ICT suites and near all classroom computers.
- All members of staff are responsible for explaining and reinforcing the rules.
- We inform all members of staff of the possible misuses of on-line access and their responsibility towards the children.
- All staff are aware of the need to report any misuse.

Acceptable Use Policy (AUP) for KS1 PUPILS

Learner Acceptable Use Agreement Template

My Name is_______________________________________

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet
- I will keep my password for the computers/Purple Mash safe and only share them with adults I trust in school and at home

Signed (child): ....

____

Acceptable Use Policy (AUP) for KS2 PUPILS

This agreement will help keep me safe and help me to be fair to others

1. ***I learn online*** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. School internet and devices are monitored.
2. ***I ask permission*** – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.
3. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things, and I remember my online safety rules.
4. ***I am a friend online*** – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.
5. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
6. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes add-ons can cost money, so it is important I always check for these too.
7. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
8. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
9. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
10. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
11. ***I check with an adult before I meet an online friend*** face to face for the first time, and I never go alone.
12. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
13. ***I keep my body to myself online*** – I never get changed or show what's under my clothes in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.
14. ***I say no online if I need to*** – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.

15. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
16. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
17. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
18. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour.
19. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
20. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
21. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
22. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find.

~~~~~~~~~~~~~~~~~~~~

I have read and understood this agreement.

If I have any questions, I will speak to a trusted adult: at school that includes ____.

Outside school, my trusted adults are____________________________________

Signed: _________________________ **Date: ____________________**
~~~~~~~~~~~~~~~~~~~~

Northwick Park Academy Trust Acceptable Usage agreement for Staff

What is an AUP?

We ask all children, young people and adults involved in the life of Northwick Park Academy Trust to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and I will be asked to sign it upon entry to the school and every time changes are made.

Why do we need an AUP?

All staff, governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy.

Where can I find out more?

All staff, governors and volunteers should read Northwick Park Academy Trust's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).

If you have any questions about this AUP or our approach to online safety, please speak to Tracy Smith or Jenny Stevenson.

What am I agreeing to?

1. I have read and understood Northwick Park Academy Trust's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
2. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Head teacher (if by an adult).
3. I understand the responsibilities listed for my role in the school's Online Safety policy (staff please note that the 'all staff' section applies as well as any other category) and agree to abide by these.
4. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices (regardless of time, location or internet connection) and networks/platforms/internet/other technologies, including encrypted content, is monitored/captured/viewed by these systems and/or relevant/authorised staff members.

5. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:
    - not sharing other's images or details without permission
    - refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
6. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames on different platforms) in any way other than school-approved and school- monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the head teacher.
7. Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety. If I am not sure if I am allowed to do something in or related to school, I will not do it.
8. I understand the importance of upholding my online reputation, my professional reputation and that of the school and Trust, and I will do nothing to impair either. More guidance on this point can be found in this Online Reputation guidance for schools and in Northwick Park Academy Trust social media policy/guidance.
9. I agree to adhere to all provisions of the school Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify Elaine Rising or Sharon Rosher if I suspect a breach. I will not store school- related data on personal devices, storage or cloud platforms. USB keys, where allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
10. I will use school devices and networks/internet/platforms/other technologies for school business and I will never use these to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
11. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
12. I understand and support the commitments made by pupils, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.
13. I will follow the guidance in the Online Safety Policy for reporting incidents – I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture. I have read the sections on handing incidents and concerns about a child in general, sexting, upskirting, bullying, sexual violence and harassment, misuse of technology and social media.
14. I understand that breach of this AUP and/or of the school's full Online Safety Policy here may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: ______________________________

Name: ______________________________

Role: ______________________________

Date: ______________________________

To be completed by Tracy Smith (online Safety Lead for the Northwick Park Academy Trust

I approve this user to be allocated credentials for school systems as relevant to their role.

Signature: ______________________________

Name: ______________________________

Role: **Online Safety Lead**

Date: ______________________________

Acceptable Use Policy (AUP) for PARENTS

What is an AUP?

We ask all children, young people and adults involved in the life of Northwick Park Academy Trust to sign an Acceptable Use* Policy (AUP), which is a document that outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Your child has also signed an AUP which has been sent home.

Why do we need an AUP?

These rules have been written to help keep everyone safe and happy when they are online or using technology. Sometimes things go wrong and people can get upset, but these rules should help us avoid it when possible, and be fair to everybody.

School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep your children safe.

We tell your children that they should not behave any differently when they are out of school or using their own device or home network. What we tell pupils about behaviour and respect applies to all members of the school community:

“Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face.”

Where can I find out more?

You can read Northwick Park Academy Trust’s full Online Safety Policy on the school website for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc). If you have any questions about this AUP or our approach to online safety, please speak to Mrs Smith, Mrs Gravely, Mrs Rising or Mrs Rosher.

What am I agreeing to?

1. I understand that Northwick Park Academy Trust uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.
2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
3. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school.
4. I will promote positive online safety and model safe, responsible and positive behaviours in my 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 the school staff, volunteers, governors, contractors, pupils or other parents/carers.
5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.
6. I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant form.
7. I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety. Understanding human behaviour is more helpful than knowing how a particular app, site or game works.
8. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK.
9. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children.
10. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
11. I can find out more about online safety at Northwick Park Academy Trust by reading the full Online Safety Policy and can talk to staff if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.
12. I will not use private groups, the school's Facebook page, or personal social media to complain about or criticise the school or members of its staff, or address behaviour issues with other

pupils. This is not constructive and the school can’t improve or address issues if they aren’t raised in an appropriate way.

Acceptable Use Policy (AUP) for PARENTS

~~~~~~~~~~~~~~~~~~~~~

I/we have read, understood and agreed to this policy.

Signature/s: ____

Name/s of parent / guardian: ____

Parent / guardian of: ____

Date: ____
~~~~~~~~~~~~~~~~~~~~~

Northwick Park Academy Trust

Infringements Policy

At Northwick Park Academy Trust we take every measure to ensure that all ICT technologies including the internet are used effectively and appropriately. However there maybe occasions when incidents of mistreatment occur. This mistreatment of such technologies applies to both teaching and non- teaching staff, students and visitors as well as children.

All incidents, minor or major, are monitored by the Trust Online Safety Co-ordinator Tracy Smith and by the school based Online Safety leads – Tracy Smith (LB), Jenny Stevenson (NP), Elaine Rising (NP) or Sharon Rosher (LB) and the System Administrators to identify any trends in pupil behaviour. They then ensure they respond appropriately in line with the school guidelines. All incidents are recorded within a log which is kept with the system administrators.

Minor Incidents

This include:-

- downloading materials or images not relevant to their studies, in direct breach of the school’s acceptable use policy
- misconduct associated with student logins, such as using someone else’s password
- incidents involving pupils using their own technology in school, such as leaving a mobile phone turned on or using it in class, sending nuisance text messages, or the unauthorised taking of images with a mobile phone camera, still or moving.

For the majority of these minor incidents the pupil(s) concerned will be given a warning and the incident recorded. If the behaviour is repeated or escalates then there is evidence to support a more serious response.

The Online Safety Co-ordinators monitor all minor incidents to identify trends in behaviour and responds proactively via offering additional training for staff and information for children.

Inappropriate materials or activities

Due to the nature of the internet there will be some material that is just not appropriate within the school environment. Examples might include soft-core pornography, hate material, drug or bomb-making recipes, or material that others may find offensive such as sexist or racist jokes, cartoons, or material which is used in low-level harassment.

Such incidents are:-

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites
- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging or social networking sites
- Accidentally corrupting or destroying others' data without notifying a member of staff of it

- Accidentally accessing offensive material and not using the Hector Protector or notifying a member of staff of it

The suggested ways of dealing with these incidents are

1. Play the situation down; don’t make it into a drama.
2. Report to the head teacher/online safety officer and decide whether to inform parents of any children who are involved.
3. Inform the school technicians and ensure any sites are filtered
4. Inform the LA or the service provider E$_2$BN.
5. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.

Incidents Involving Others.

Incidents which involve others are of a more serious nature. For example incidents of bullying using e-mail or mobile technology. Also

- Deliberately corrupting or destroying someone’s data, violating privacy of others
- Sending an email or message via Social media that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material
- Continued sending of emails or Social Media messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

Suggested ways of dealing with these incidents are:-

1. Advise the child not to respond to the message.
2. Refer to relevant policies including Online Safety anti-bullying and PHSE and apply appropriate sanctions.
3. Inform and request the comments be removed if the site is administered externally.
4. Secure and preserve any evidence.
5. Inform the sender’s e-mail service provider.
6. Notify parents of the children involved.
7. Consider delivering a parent workshop for the school community.
8. Inform the police if necessary.
9. Inform the LA Online Safety officer.
10. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
11. Endeavour to trace the origin and inform police as appropriate.

Incidents involving a member of staff

Any incident involving a member of staff is a serious, and often complex, matter. There may be implications for the safety of pupils, fellow employees and the learning environment, and for the reputation of the school. As a school, we have a robust Acceptable Use Policy in place which all staff are expected to read and sign.

In incidents of this nature we follow the disciplinary protocols set out in our anti-bullying, behaviour management and sanctions policies and ensure that the appropriate authorities are informed. Those involved are then given the appropriate support and counselling.

Incidents involving illegal materials and activities

These incidents within school are very rare but relate to indecent images and serious harassment and stalking (as defined under section 7 of the Protection of Children's Act 1978 and Protection of Harassment Act 1997). Due to the seriousness of the situation incidents involving indecent materials should always be reported to the police immediately, legal advice sought in relation to disciplinary action and prepare staff, children and equipment for the following investigation.
If an incident of this seriousness arises we, as a school, will conduct a full review of all Online Safety policies and procedures, equipment and network with the possibility of a full diagnostic audit of all equipment and network areas. All staff will be debriefed to ensure full co-operation and insight into these issues to ensure that it is never repeated.

Misuse and misconduct by staff

To fully ensure the safety of the children and school the staff are also subject to guidance regarding incidents.

Such incidents are -

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Statuses or comments on Social Media which have any relation to the school, nature of the job, classes or children which aren't on the 'closed school' pages.
- Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
- Not implementing appropriate safeguarding procedures.
- Any behaviour on the World Wide Web that compromises the staff members' professional standing in the school and community.
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on network.
- Serious misuse of, or deliberate damage to, any school hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

Should incidents of this nature occur we will

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment by an outside agency, such as the school's ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they may be instantly suspended. There is liable to be an investigation before disciplinary action is taken for any alleged offence.

As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

If, as a Trust, we believe that it is necessary we will involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, and the Local Authority Human Resources team.

How will Staff and children be informed of procedures?

At Northwick Park Academy Trust we will inform all parties concerned about the infringements and sanctions.

- They will be fully explained and included within the school's Online Safety / Acceptable Use Policy. All staff will be required to sign the school's Acceptable Use Policy acceptance form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate Online Safety / acceptable use form;
- The school's Online Safety policy will be made available and explained to parents, and parents will sign an acceptance.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.

Northwick Park Academy Trust

Mobile Phone Policy

1. Introduction and aims

At Northwick Park Academy Trust we recognise that mobile phones, including smart phones, are an important part of everyday life for our pupils, parents and staff, as well as the wider school community.

Our policy aims to:

- Promote, and set an example for, safe and responsible phone use
- Set clear guidelines for the use of mobile phones for pupils, staff, parents and volunteers
- Support the school's other policies, especially those related to child protection and behaviour

This policy also aims to address some of the challenges posed by mobile phones in school, such as:

- Risks to child protection
- Data protection issues
- Potential for lesson disruption
- Risk of theft, loss, or damage
- Appropriate use of technology in the classroom

2. Roles and responsibilities

2.1 Staff

All staff (including teachers, support staff, and supply staff) are responsible for enforcing this policy.

Volunteers, or anyone else otherwise engaged by the school, must alert a member of staff if they witness, or are aware of, a breach of this policy.

The Head teacher and Online Safety Lead are responsible for monitoring the policy every year, reviewing it, and holding staff and pupils accountable for its implementation.

2.2 Governors

Our Trustees and individual school Chairs of Governors are responsible for overseeing this policy and how it is monitored and implemented within school.

3. Use of mobile phones by staff

3.1 Personal mobile phones

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to make or receive calls, send texts, or access social media, while children are present. 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).

There may be circumstances in which it's appropriate for a member of staff to have use of their phone during contact time. For instance:

- For emergency contact by their child, or their child's school
- In the case of acutely ill dependents or family members

The head teacher will decide on a case-by-basis whether to allow for special arrangements. It may also be deemed necessary by the Head teacher that members of SLT have mobile phones for use if she is not in the school building as a point of contact.

If special arrangements are not deemed necessary, school staff can use the school office number as a point of emergency contact.

3.2 Data protection

Staff must not use their personal mobile phones to process personal data, or any other confidential school information.

This includes using personal mobile devices for taking photographs or videos within school or when accompanying any school visits.

3.3 Safeguarding

Staff must refrain from giving their personal contact details to parents or pupils, including connecting through social media and messaging apps.

Staff must avoid publicising their contact details on any social media platform or website, to avoid unwanted contact by parents or pupils. Our social media accounts are monitored by members of Senior Leadership and can be contacted accordingly.

Staff must not use their mobile phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil. If it's necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done by using school cameras or iPads only.

3.4 Using personal mobiles for work purposes

In some circumstances, it may be appropriate for staff to use personal mobile phones for work. Such circumstances may include, but aren't limited to:

- Emergency evacuations
- Supervising off-site trips
- Supervising residential visits

In these circumstances, staff will:

- Use their mobile phones in an appropriate and professional manner, in line with our staff code of conduct
- Not use their phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil
- Refrain from using their phones to contact parents. If necessary, contact must be made via the school office

3.5 Sanctions

Staff that fail to adhere to this policy may face disciplinary action.

See the school's staff disciplinary policy for more information.

4. Use of mobile phones by pupils

Once children reach upper Key Stage two we allow but discourage children to bring a mobile to school, in certain circumstances. For instance

- Travelling to school by themselves
- Young carers who need to be contactable

If pupils are bringing mobile phones to school they are not allowed to access them or use them. All phones must be handed into the school office at the start of the day and it is the child's responsibility to collect it at the end of the day.

Pupils must adhere to the school's acceptable use agreement for mobile phone use (see appendix 1).

4.1 Sanctions

If a pupil is in breach of this policy.

- The phones will be confiscated (Schools are permitted to confiscate phones from pupils under sections 91 and 94 of the Education and Inspections Act 2006)
- If a phone is confiscated, depending upon the circumstances pupils will be allowed to collect it from the head teacher's office at the end of the day. If the circumstances are more serious, the phone will be handed to a parent once arrival at the school.

If the DSL or OSL have significant cause for concern over a child's behaviour or well-being, staff have the power to search pupils' phones, as set out in the DfE's guidance on searching, screening and confiscation. The DfE guidance allows you to search a pupil's phone if you have reason to believe the phone contains pornographic images, or if it is being/has been used to commit an offence or cause personal injury.

If it is found that evidence found on a mobile device is of significant concern e.g. phone contains pornographic images, or if it is being/has been used to commit an offence or cause personal injury the process for recording safeguarding concern and reporting such issues will be followed leading to the sanctions outlined in the Infringements policy.

Certain types of conduct, bullying or harassment can be classified as criminal conduct. The school takes such conduct extremely seriously, and will involve the police or other agencies as appropriate.

Such conduct includes, but is not limited to:

- Sexting
- Threats of violence or assault
- Abusive calls, emails, social media posts or texts directed at someone on the basis of someone's ethnicity, religious beliefs or sexual orientation

5. Use of mobile phones by parents, volunteers and visitors

Parents, visitors and volunteers (including governors and contractors) must adhere to this policy as it relates to staff if they are on the school site during the school day.

This means:

- Not taking pictures or recordings of pupils, unless it's a public event (such as a school fair), or of their own child
- Using any photographs or recordings for personal use only, and not posting on social media without consent
- Not using phones in lessons, or when working with pupils

Parents, visitors and volunteers will be informed of the rules for mobile phone use when they sign in at reception or attend a public event at school.

Parents or volunteers supervising school trips or residential visits must not:

- Use their phone to make contact with other parents
- Take photos or recordings of pupils, their work, or anything else which could identify a pupil

Parents or volunteers supervising trips are also responsible for enforcing the school's policy for pupils using their phones, as set out in section 4 above.

Parents must use the school office as the first point of contact if they need to get in touch with their child during the school day. They must not try to contact their child on his/her personal mobile during the school day.

6. Loss, theft or damage

Pupils bringing phones to school must ensure that phones are appropriately labelled, and are stored securely in the school office when not in use.

Pupils must secure their phones as much as possible, including using passwords or pin codes to protect access to the phone's functions. Staff must also secure their personal phones, as well as any work phone provided to them. Failure by staff to do so could result in data breaches.

All schools continue with:

The school accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while pupils are travelling to and from school.

Confiscated phones will be stored in the school office or Mrs Lane's Office in a locked drawer.

If a phone or mobile device is confiscated the Northwick Park Academy Trust becomes responsible for the phone, and can be held responsible for loss, theft, or damage.

Lost phones should be returned to the school office. The school will then attempt to contact the owner.

7. Monitoring and review

The school is committed to ensuring that this policy has a positive impact of pupils' education, behaviour and welfare. When reviewing the policy, the school will take into account:

- Feedback from parents and pupils
- Feedback from teachers
- Records of behaviour and safeguarding incidents
- Relevant advice from the Department for Education, the local authority or other relevant organisations

8. Appendix 1: Acceptable use agreement for pupils

Acceptable use agreement

You must obey the following rules if you bring your mobile phone to school:

1. You may not use your mobile phone during lessons, unless the teacher specifically allows you to.
2. Phones must be switched off (not just put on 'silent').
3. You must hand your phone into a member of staff in the school office. It is your responsibility to collect it at the end of the day.
4. You may not use your mobile phone in the toilets or changing rooms. This is to protect the privacy and welfare of other pupils.
5. You cannot take photos or recordings (either video or audio) of school staff or other pupils without their consent.
6. Avoid sharing your contact details with people you don't know, and don't share other people's contact details without their consent.
7. Don't share your phone's passwords or access codes with anyone else.
8. Don't use your mobile phone to bully, intimidate or harass anyone. This includes bullying, harassing or intimidating pupils or staff via:
    a. Email
    b. Text/messaging app
    c. Social media
9. Don't use your phone to send or receive anything that may be criminal.
10. Rules on bullying, harassment, and intimidation apply to how you use your mobile phone even when you aren't in school.
11. You must comply with a request by a member of staff to switch off, or turn over, a phone. Refusal to comply is a breach of the school's behaviour policy and will be dealt with accordingly.

Social Media Policy

Northwick Park Academy Trust's SM presence

Northwick Park Academy Trust works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online (Mumsnet is a favourite).

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

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.

Tracy Smith and Lynne Keys are responsible for managing our Facebook accounts and checking our Wikipedia and Google reviews. They follow the guidance in the Safer Internet Centre online-reputation management document here.

Staff, pupils' and parents' SM presence

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

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

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

Many social media platforms have a minimum age of 13, but the schools regularly deal with issues arising on social media with pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

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

Parents can best support this (as outlined on p.15) by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to introduce the Children's Commission Digital 5 A Day (see appendix 8).

It is encouraging that 73% of pupils trust their parents on online safety (although only half talk about it with them more than once a year at the moment).

The school has an official Facebook account (managed by Tracy Smith and Lynne Keys) and will respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children.

Email is the official electronic communication channel between parents and the school, and between staff and pupils).

Pupils/students are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

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

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

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

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

The serious consequences of inappropriate behaviour on social media are underlined by the fact that of the 131 Prohibition Orders issued to staff in 2017, 73 involved social media/technology (and 27 of the 66 orders by August 2018).

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video (see page 25) and permission is sought before uploading photographs, videos or any other information about other people.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

Social media incidents

Breaches of this policy and of school AUPs (Acceptable Use Policies) will be dealt with in line with the school behaviour policy (for pupils) or code of conduct (for staff).

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

Where an offending post has been made by a third party, the school may report it to the platform where it is hosted, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process. The police or other authorities may be involved where a post is potentially illegal or dangerous.

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature by the school. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

Further questions

If parents have further questions, they can contact the DSL or OSL at the school; the NSPCC has a parent online safety helpline which can help with general issues that are not school specific.

Staff should speak to a member of the SLT in the first instance, who may then call on the expertise of local authority advisers or Professionals' Online-Safety Helpline (from UK SIC).

Children's COMMISSIONER

Digital 5 a day

Easy to follow, practical steps for children and parents to achieve a healthy and balanced digital diet

The **digital 5 a day** provides a simple framework that reflects the concerns of parents/ carers as well as children's behaviours and needs. It can also act as a base for family agreements about internet and digital device use throughout both the holidays and term time.

Based on the NHS's evidence-based ''five steps to better mental wellbeing', the digital 5 a day campaign gives children and parents easy to follow, practical steps to achieve a healthy and balanced digital diet.

1. Connect

The internet has enabled everyone to maintain friendships and family relationships no matter where they are in the world and children often say that chatting with friends is the best thing about social media.

It's important to acknowledge that this is how children keep in touch but it's also important to have a conversation with them about who they are connecting with and their privacy settings. Remember to keep a dialogue open and talk to your child to understand how they're spending their time and so that they can come to you for help should they need to.

2. Be active

Activity is very important for mental wellbeing and all children should have time to switch off and get moving.

Children don't have to be an athlete to be active. Find something that they enjoy – be that swimming, walking, dancing or yoga – begin at a level that works for them and make it a regular activity.

Researching an activity or place online before going out is a good way of combining the two and provides an opportunity for you to use the internet together.

3. Get creative

The internet provides children with unlimited opportunities to learn and to be creative. From learning to code to building complex structures in Minecraft to creating video content, the summer can be a great opportunity for children to build their digital skills. Time spent online doesn’t have to be spent passively consuming content. It can be educational, creative and can provide opportunities to build skills for later life.

4. Give to others

As well as using the internet to learn about how to get involved with local and national charitable schemes, children can give to others through their everyday activities.

Remind children that by giving positive feedback and support to friends and family as well as reporting the negative behaviour of others, children can help the web make a positive place for everyone.

5. Be mindful

We hear that children often feel pressured by the constantly connected nature of the internet. While they might want to do other things, it can be difficult for them to put their phones down when apps are encouraging them to engage. Being mindful about the amount of time that your child is spending online – and encouraging them to be mindful about how this makes them feel – is important.

Encourage children to come up with ways of managing this i.e. keeping a diary as way of logging the amount of time they are spending online or downloading an app that helps them manage their notifications.

Northwick Park Academy Trust

Internet Policy

At Northwick Park Academy Trust we understand that the Internet is an essential element in 21st century life for education. ICT skills and knowledge are vital to access life-long learning and employment. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet provides many benefits to pupils and the professional work of staff through, for example:

- access to world-wide educational resources, including museums and art galleries;
- access to experts in many fields for pupils and staff;
- educational and cultural exchanges between pupils world-wide;
- collaboration between pupils, professionals and across sectors;
- access to learning wherever and whenever convenient.

Due to the nature of the Internet we at Northwick Park Academy Trust are aware that the Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource as well as a potential risk to young and potentially vulnerable people.

In line with our other policies that are in place to protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This must be within a 'No Blame', supportive culture if pupils are to report abuse. Risks can be high outside school, so in response to this we offer information as part of an education programme to support parents and carers to protect their children.

To protect the children, staff, school and network to the fullest we access technical and infrastructure support.

Our school :-

- Maintains the filtered broadband connectivity through E$_2$BN;
- Works in partnership with the LA to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Has additional user-level filtering in-place
- Ensures network health through appropriate anti-virus software etc and network set-up so staff and pupils cannot download executable files such as .exe / .com / .vbs etc.;
- Ensures their network is 'healthy' by having LA health checks annually on the network;
- Utilises caching as part of the network set-up;
- Ensures the Systems Administrator is up-to-date with available services and policies;
- Ensures the Systems Administrator checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;

- Never allows pupils access to Internet logs;
- Uses 'Hector Protector' which pupils can activate should they find something on their screen which makes them feel uncomfortable;
- Uses individual log-ins for all pupils from Reception age and all other users;

- Never sends personal data over the Internet unless it is encrypted or otherwise secured. This includes the use of county stored data using target tracker, which is password protected within school and governed by the LA's data protection guidance,
- Never allows personal level data off-site unless it is on an encrypted device;
- Uses 'safer' search engines with pupils such as http://yahooligans.yahoo.com/ | http://www.askforkids.com/ and activates 'safe' search where appropriate;

Where the internet is concerned we believe that supervision is the key. Aimless surfing is discouraged and children are taught to use the internet in response to a need and social networking sites are completely blocked for all.

At Northwick Park Academy Trust we:-

- Supervise pupils' use at all times, as far as is reasonable, and are vigilant in learning resource areas where older pupils have more flexible access;
- Use the E_2BN filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- Have additional user-level filtering, so adapt filtering to the age of the pupils;
- Encourage staff to preview all sites before use (where not previously viewed and cached) or only use sites accessed from managed 'safe' environments,
- Plan the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- Are vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Inform users that Internet use is monitored;
- Inform staff and students that that they must report any failure of the filtering systems directly to the System Administrator or Mrs Smith. Our systems administrators report to LA where necessary;
- Only uses approved or checked webcam sites;
- Has blocked pupil access to music download or shopping sites
- Requires pupils (and their parent/carer) from Year R, and Key Stage 1, to individually sign an e-safety and acceptable use agreement form which is fully explained and used as part of the teaching programme;

This policy works hand in hand with our Online safety policy and in order to address the important point raised in both of these documents regarding the safety and integrity of the children, staff and school we ensure that the joys and dangers of the internet and remaining safe are built into the discrete ICT sessions and every other curriculum area where ICT is used.

E-Security Policy

Strategic and operational practices

At the Northwick Park Academy Trust:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Sarah Colquhoun is the Data Protection Officer (DPO) with responsibility for data protection compliance.
- Staff are clear who the key contact(s) for key school information are (the Information Asset Owners). We have listed the information and information asset owners.
- We ensure staff know to immediately report, and who to report to, any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices are lost or stolen, so that relevant action(s) can be taken.
- All staff are DBS checked and records are held in one central record.

  We ensure ALL the following school stakeholders sign an Acceptable Use Agreement. We have a system so we know who has signed.

  - staff
  - governors
  - pupils
  - parents
  - volunteers

  This makes clear all responsibilities and expectations with regard to data security.
- We have approved educational web filtering across our wired and wireless networks. We also have an additional layer of monitoring software across our network system. We monitor school e-mails / blogs / online platforms, etc. to ensure compliance with the Acceptable Use Agreement. As well as monitoring usage, we may also monitor content of e-mails / blogs / etc.
- We follow Academy guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.
- We require staff to use STRONG passwords for access into our MIS system>.
- We require that any personal/sensitive material must be encrypted if the material is to be removed from the school, and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff who set up usernames and passwords for e-mail, network access, and other online services, work within the approved system and follow the security processes required by those systems.
- We ask staff to undertake house-keeping checks at least annually to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical or manual solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 mins. idle time.

- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to DfE / other schools.
- We use Egress to transfer documents to schools, such as references, reports of children.
- We use Microsoft Cloud for online document storage.
- We store any sensitive/special category written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any back-up tapes in a secure, fire-proof cabinet. Back-ups are encrypted. No back-up tapes leave the site on mobile devices.
- We comply with the WEEE directive on equipment disposal, by using an approved disposal company for disposal of IT equipment. For systems, where any protected or restricted data has been held, (such as servers, photocopiers), we get a certificate of secure deletion.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using a cross-cut shredder or destroyed by a confidential waste company.

Legislation

The Northwick Park trust are aware of the legislative framework under which this online safety policy and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

A useful summary of relevant legislation can be found at: Report Harmful Content: Laws about harmful behaviours

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.
-

The Trust has viewed the National Crime Agency website which includes information about "Cyber crime – preventing young people from getting involved". Each region in England (& Wales) has a Regional Organised Crime Unit (ROCU) Cyber-Prevent team that works with schools to encourage young people to make positive use of their cyber skills.

There is a useful summary of the Act on the NCA site.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.

- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of learners when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/learnersupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The School Information Regulations 2012

Requires schools to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the Revenge Porn Helpline

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/

South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/

Childnet – http://www.childnet-int.org/

Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline

Revenge Porn Helpline - https://revengepornhelpline.org.uk/

Internet Watch Foundation - https://www.iwf.org.uk/

Report Harmful Content - https://reportharmfulcontent.com/

Harmful Sexual Support Service

CEOP

CEOP - http://ceop.police.uk/

ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources

Kent – Online Safety Resources page

INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/

UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Tools for Schools / other organisations

Online Safety BOOST – https://boost.swgfl.org.uk/

360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

360Data – online data protection self-review tool: www.360data.org.uk

SWGfL Test filtering - http://testfiltering.com/

UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework

SWGfL 360 Groups – online safety self review tool for organisations working with children

SWGfL 360 Early Years - online safety self review tool for early years organisations

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/

SELMA – Hacking Hate - https://selma.swgfl.co.uk

Scottish Anti-Bullying Service, Respect me - http://www.respectme.org.uk/

Scottish Government - Better relationships, better learning, better behaviour -

http://www.scotland.gov.uk/Publications/2013/03/7388

DfE - Cyberbullying guidance -

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit:

http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit

Childnet – Project deSHAME – Online Sexual Harassment

UKSIC – Sexting Resources

Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk

UKCCIS – Education for a connected world framework

Department for Education: Teaching Online Safety in Schools

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool
ICO Guides for Organisations
IRMS - Records Management Toolkit for Schools
ICO Guidance on taking photos in schools

Professional Standards/Staff Training

DfE – Keeping Children Safe in Education

DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet – School Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support/Cyber-security

UKSIC – Appropriate Filtering and Monitoring

SWGfL Safety & Security Resources

Somerset - Questions for Technical Support

SWGfL - Cyber Security in Schools.

NCA – Guide to the Computer Misuse Act

NEN – Advice and Guidance Notes

Working with parents and carers

SWGfL – Online Safety Guidance for Parents & Carers

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops/education

Internet Matters

Prevent

Prevent Duty Guidance
Prevent for schools – teaching resources
Childnet – Trust Me

Research

Ofcom –Media Literacy Research

Ofsted: Review of sexual abuse in schools and colleges

Further links can be found at the end of the UKCIS Education for a Connected World Framework

Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MAT	Multi Academy Trust
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework