HARLINGTON SCHOOL

## GDPR Digital Safeguarding Policy

| | |
|---|---|
| Reviewed and update: | June 2019 |
| Next review: | Annually |
| Status: | Statutory |

### What is this policy?

Digital safety is an integral part of safeguarding. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2018 (KCSIE) and other statutory documents; it is designed to sit alongside Harlington School's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

### The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Harlington School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

### Who is the lead contact for Digital safety?

Mr I Wells (Assistant Headteacher) is Harlington Schools Digital Safeguarding lead. Digital Safeguarding issues can be brought to Mr Wells, but KCSIE makes clear that "the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."

### What are the main online safety risks today?

Online-safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct (identified by Professor Tanya Byron's 2008 report "Safer children in a digital world"). They do not stand in isolation, however, and it is important to understand the interplay between all three.

### The main areas of risk for our school community can be summarised as follows:

**Content**

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate content including incitement
- Content validation: how to check authenticity and accuracy of online content

**Contact**

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

**Conduct**

- Aggressive behaviours (bullying, trolling, etc)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (Internet or gaming), gambling, body image, etc)
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

**How will this policy be communicated?**

This policy will be communicated in the following ways:

- Posted on the school website
- Available on the internal staff network/drive
- Part of school 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 Agreement  s (AUAs) for staff, volunteers, contractors, governors, students and parents/carers.
- AUAs issued to whole school community, on entry to the school, 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, students and other stakeholders, helping to ensure further engagement

**Overview**

**Aims**

This policy aims to:

- Set out expectations for all Harlington School'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 school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school 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 school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

### Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with Harlington's Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and normally the headteacher will handle referrals to the LA designated officer (LADO).

We reference amongst other sources the help materials collated by London Grid for Learning at https://reporting.lgfl.net. This includes links to external support and helplines for both students 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 might be useful to share with parents, and anonymous support for children and young people.

### Scope

This policy applies to all members of the Harlington School's community (including staff, governors, volunteers, contractors, students/students, 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.

### Roles and responsibilities

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

### Headteacher/Principal – Ms E Horrigan

**Key responsibilities:**

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the 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 Children Board (LSCB) guidance
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school'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 Harlington implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident

- Ensure suitable risk assessments are undertaken so the curriculum meets needs of students, 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 Harlington's arrangements for online safety
- Ensure the school website meets statutory DfE requirements

**Designated Safeguarding Lead / Digital Safeguarding Lead – Mrs A Maidment / Mr I Wells**

**Key responsibilities** The DSL can delegate certain online-safety duties, e.g. to the Digital Safeguarding Lead, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education 2018:

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."
- Where the Digital Safeguarding Lead is not the named DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised.
- Ensure "An effective approach to online safety that empowers our school to protect and educate the whole school in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with the local authority and work with other agencies in line with Working together to safeguard children".
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- Work with the Headteacher, DPO 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.
- Review and update this policy, other online safety documents (e.g. Acceptable use Agreement s) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends.
- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life.
- Promote an awareness and commitment to online safety throughout Harlington School's community, with a strong focus on parents, including hard-to-reach parents.
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT and the designated online safety governor to discuss current issues, review incident logs and filtering/change control logs and discuss how issues that may arise.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Oversee and discuss 'appropriate filtering and monitoring' with governors and ensure that staff are aware.
- Ensure the 2018 Department for Education guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff.

**Safeguarding Link Governor –Ms C Mosdell**

**Key responsibilities (quotes are taken from Keeping Children Safe in Education 2018):**

- Approve this policy and strategy and subsequently review its effectiveness.
- "Ensure an appropriate senior member of staff, from the school's leadership team, is appointed to the role of DSL with lead responsibility for safeguarding and child protection (including online safety).
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the Digital Safeguarding lead / DSL. Incorporate online safety into standing discussions of safeguarding at governor meetings.
- Where the Digital Safeguarding Lead is not the named DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, the school's Data Protection Lead, DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction and regularly updated. Ensure that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach."
- "Ensure appropriate filters and appropriate monitoring systems are in place whilst taking care to ensure that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding".
- "Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum.

**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 that the Designated Safeguarding Lead (DSL) is Mrs A Maidment and Digital Safeguarding Lead is Mr I Wells.
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school 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 Agreement .
- Notify the Designated Safeguarding Lead / Digital Safeguarding Lead if the policy does not reflect practice in Harlington. Follow escalation procedures if concerns are not promptly acted upon.
- 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 students).
- 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

students/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).

- To carefully supervise and guide students 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.
- Encourage students/students to follow their Acceptable use Agreement , remind them about it and enforce school sanctions.
- Notify the DSL/ Digital Safeguarding Lead 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
- Model safe, responsible and professional behaviours in your own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

**PSHE Lead**

**Key responsibilities from September 2019 for September 2020 (quotes taken from DfE press release on 19 July 2018 on New relationships and health education in schools):**

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / RE / RSE curriculum, "complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds."
- Work closely with the DSL/ Digital Safeguarding Lead and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RE / RSE

**Computing Curriculum Lead – Mr W McGovern**

**Key responsibilities:**

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.
- Ensure relevant whole school digital safeguarding procedures are supported through the curriculum delivery.
- Work closely with the DSL/ Digital Safeguarding Lead and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.

**Curriculum 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 students alike
- Consider how the UKCCIS framework Education for a Connected World can be applied in your context
- Work closely with the DSL/ Digital Safeguarding Lead and all other staff to ensure an understanding of the issues, approaches and messaging within Computing

**Network Manager/technician – Mr G Mullis**

**Key responsibilities:**

- As listed in the 'all staff' section, plus:
- Keep up to date with the school's Digital Safeguarding 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 / Digital Safeguarding Lead / data protection officer / LGfL TRUSTnet nominated contact to ensure that school systems and networks reflect school 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/ Digital Safeguarding Lead and senior leadership team.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online-safety related issues that come to their attention in line with school policy.
- Manage the school'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 school technology, online platforms and social media presence that any misuse/attempted misuse is identified and reported in line with school policy.

**Data Protection Officer (DPO) – GDPR Sentry Limited**

**Key responsibilities:**

- To support Harlington to ensure GDPR and Data Protection Act 2018 compliant.
- To support the data protection and safeguarding agendas identified in the key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (April 2018).
- Work with the DSL/ Digital Safeguarding Lead, headteacher and governors to ensure frameworks, processes and policies 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

**LGfL TRUSTnet Nominated contacts – Ms E Horrigan, Mr G Mullis, Mr M SahotaSahota Sahota Sahota**

**Key responsibilities:**

- To ensure all LGfL TRUSTnet services are managed on behalf of the school in line with school policies, following data handling procedures as relevant
- Work closely with the DSL/ Digital Safeguarding Lead and DPO to ensure they understand who the nominated contacts are and what they can do / what data access they have, as well as the implications

of all existing services and changes to settings that you might request – e.g. for YouTube restricted mode, internet filtering settings, firewall port changes, student email settings, and sharing settings for any cloud services such as Microsoft Office 365 and Google G Suite.

- Ensure the DPO is aware of the GDPR information on the relationship between the school and LGfL TRUSTnet

**Volunteers and contractors**

**Key responsibilities:**

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

**Students**

**Key responsibilities:**

- Read, understand, sign and adhere to the student Acceptable use Agreement 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 school's Acceptable use Agreement 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 school's parental Acceptable use Agreement (AUA) and read the student AUA and encourage their children to follow it
- Consult with the school if they have any concerns about their children's use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: 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, students or other parents/carers.

**Education and curriculum**

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- PSHE
- Health Education, Relationships and Sex Education
- Computing

- Citizenship

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 students)

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in Harlington or setting as homework tasks, all staff should encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).

Equally, all staff should carefully supervise and guide students when engaged in learning activities involving online technology (including, extra-curricular and extended school activities), 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 Harlington 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 the UK Council for Child Internet Safety.

Annual reviews of curriculum plans / schemes of work (including for SEND students) 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**

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, Citizenship and Relationships and Sex Education).

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 Digital Safeguarding lead / Designated Safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Non-teaching 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).

Harlington procedures for dealing with online-safety will be mostly be detailed in the following policies:

- Safeguarding and Child Protection Policy
- Sexual Harassment Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable use Agreements

- Prevent Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school 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 students when they come into school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the Digital Safeguarding 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 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).

The school will actively seek support from other agencies as needed. We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or students engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law including Prevent concerns and safeguarding issues such as sexting.

**Sexting**

Harlington refers to the UK Council for Child Internet Safety (UKCCIS) guidance on sexting ('youth produced sexual imagery') in schools. We recognise that  where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview 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 Digital Safeguarding 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 school DSL will in turn use the full 50-page guidance document including case studies, typologies and a flow chart as shown below (for information only, must be viewed in the context of the full document) to decide next steps and whether other agencies need to be involved.

It is important that everyone understands that whilst sexting is illegal, students/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 school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying. Please refer to the Cyberbullying Policy for more information**.**

**Sexual violence and harassment**

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviour's 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.

The following is an excerpt Keeping Children Safe in Education (section 46 on page 21):

"As with all safeguarding concerns, it is important that in such instances staff take appropriate action in accordance with their child protection policy. They should not assume that someone else is responding to any incident or concern. If in any doubt, they should speak to the designated safeguarding lead (or a deputy). In such cases, the basic safeguarding principles remain the same, but it is important for the school or college to understand why the victim has chosen not to make a report themselves. This discussion should be handled sensitively and with the support of children's social care if required. There may be reports where the alleged sexual violence or sexual harassment involves students or students from the same school or college, but is alleged to have taken place away from the school or college premises, or online. There may also be reports where the children concerned attend two or more different schools or colleges. The safeguarding principles, and individual schools' and colleges' duties to safeguard and promote the welfare of their students and students, remain the same. The same principles and processes as set out from paragraph 48 will apply. In such circumstances, appropriate information sharing and effective multi-agency working will be especially important."

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

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

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

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

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

**Social media incidents**

See the social media section later in this document for rules and expectations of behaviour for children and adults at Harlington School. These are also governed by school Acceptable use Agreement

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

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

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

**Data protection and data security**

To avoid conflict or duplication Please refer to our Data Protection Policy and our Data Security Policy. These have been developed in response to GDPR and the Data Protection Act 2018.

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 schools' (April 2018), which the DPO and DSL will seek to apply.

The headteacher, data protection officer, data protection lead 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.

**Appropriate filtering and monitoring**

Harlington  appropriate systems of filtering and monitoring to comply with the recommendations outlined in "Keeping Children Safe in Education"

Harlington's, internet connection is provided by LGfL TRUSTnet. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen, which is made specifically to protect children in schools.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

Across the network we use NetSupport DNA to monitor and record all activities of users on our network.  This includes the provision of alert triggers that indicate inappropriate behaviour is taking place.

**Email**

Harlington uses the following email systems:

- Students at this school use the LondonMail / StudentMail system from LGfL TRUSTnet for all school emails
- Staff at this school use the StaffMail for all school emails

Both these systems are linked to the USO authentication system and are fully auditable, trackable and managed by LGfL TRUSTnet on behalf of the school. This is for the mutual protection and privacy of all staff, students and parents, as well as to support data protection.

General principles for email use are as follows:

- Email, ParentMail and Frog VLE are the only means of direct electronic communication to be used between staff and students / staff and parents (in both directions). Use of a different platform must be approved in advance by the headteacher/Data Protection lead in advance. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- Email may only be sent using the email systems identified in this policy. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or student personal data should never be sent/shared/stored on email.
    - If data needs to be shared with external agencies, USO-FX and Egress or other approved encryption systems should be used.
    - Internally, staff should use the school network, including when working from home when remote access is available via the RAV3 system. Access to sections of the school network may also become available through staff secure logins.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Students and staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but 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.

See also the social media section of this policy.

**School website**

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated has been the day-to-day responsibility of updating the content of the website to Mr I Wells & Mr M Parihar. The site is hosted by The Mustard Agency.

The Department for Education has determined information which must be available on a school website.

Requests for materials to go onto  the website have to be submitted by a member of SLT

Where staff submit information for the website, they are asked to remember:

- School have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission.
- Where student work, images or videos are published on the website, their identities are protected and full names are not published. Student images should not be saved as images with a filename that includes a student's full name.

**Cloud platforms**

Harlington adheres to the principles of the Department for Education document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'.

Harlington recognises the benefits of cloud based systems to support communication, learning and organisational efficiency. We also recognise the potential issues that may arise in safeguarding and data protection if we do not adopt full diligence when adopting cloud based systems. (Please refer to our Data Protection Policy, Data Security Policy and Data Protection Impact Assessment Policy (DPIA)).

The data protection officer, Data Protection Lead 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 schools Data Protection Team approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA which is shared with the schools DPO. Where required parental permission is sought.
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that student data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Students 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 student data
- Student images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store student 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 student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos and for what purpose (beyond internal assessment, which does not require express consent). Parents answer as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For a specific high profile image for display or publication

- For social media

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

All staff are governed by their contract of employment and the school's Acceptable use Agreement , which covers the use of mobile phones/personal equipment for taking pictures of students, and where these are stored. At Harlington, members of staff may occasionally use personal phones to capture photos or videos of students, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services (Staff need to note that many phones automatically back up photos).

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

Staff and parents are reminded regularly about the importance of not sharing without permission, due to reasons of child protection, data protection, religious or cultural reasons, or simply for reasons of personal privacy.

Harlington encourages 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).

Students 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

Students 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.

Students 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 are subject to bullying or abuse.

**Social media**

Currently Harlington School does not maintain. This may change in the future.

Harlington recognises that 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.

Negative coverage almost always causes some level of disruption. 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 even though there are no official/active school social media accounts.

**Staff, students' 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 students will use it. However, as stated in the Acceptable use Agreement  s 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, students and parents, also undermining staff morale and the reputation of the school (which is important for the students we serve).

Many social media platforms have a minimum age of 13, but the school regularly deals with issues arising on social media with 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 school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

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.

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.

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.

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 and permission is sought before uploading photographs, videos or any other information about other people.

**Device usage**

Please read the following in conjunction with Acceptable use Agreement 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 and bring your own device (BYOD) policy**

- **Students/students** are allowed to bring mobile phones in for emergency use. These maybe used during lunch break, but not when moving around the school buildings. During lessons, phones must remain turned off at all times, unless the teacher has given express permission as part of the lesson. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to a sanction in line with the schools Behaviour policy. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to students in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent. They should not be used during teaching. Student/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- **Volunteers, contractors, governors** should leave their phones 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 headteacher should be sought (the headteacher may choose to delegate this) 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 school events, please refer to the Digital images and video section of this policy.

**Trips / events away from school**

For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with students/students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the headteacher. 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 schools', the Headteacher and staff authorised by them have a statutory power to search students/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Full details of the school's search procedures are available in the Behaviour and Exclusions Policy and the protocols defined by the Department for Education.