# Hove Learning Federation Online Safety Policy

This policy was adopted on Autumn 2023
This policy is due for review on Autumn 2024

**We are committed to safeguarding and ensuring the health, safety and well-being of all pupils in accordance with safeguarding procedures and guidance for staff outlined in the school's Health and Safety, Child Protection, Security and Safeguarding policies.**

# 1. Aims, scope and principles

This Policy aims to set out expectations for all Hove Learning Federation community members' online behaviour, attitudes and activities and use of digital technology.

This will allow 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.

It will establish clear structures by which online misdemeanors will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Positive Relationships Policy, Anti-Bullying Policy or Code of Conduct for School Employees).

In addition, this will 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.

The policy will support 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

This policy applies to all members of the **Hove Learning Federation** community (including staff, Governors, volunteers, contractors, child/children, 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 school role.

## Table of Contents

| | |
|---|---|
| Designated Safeguarding Lead (DSL) team | Ben Patterson, Charlotte Wallace and Amanda Stewart |
| Online-Safety Leads | Ben Patterson, Charlotte Wallace and Amanda Stewart |
| Online-Safety / Safeguarding Link Governor | Lisa Marshall |
| Computing Leads | Ben Massey, Hannah Cutler, Kathy Bates and Matt Harper-Duffy |
| PSHE/RSHE Lead | Caroline Kemp Harris, Catrin Pierce and Rachel Dawson |
| Data Protection Officer (DPO) | James England |
| Network Manager / other technical support | Kevin Astle / BHCC ICT Schools / Rab Atmani / John Nicholson |
| Date this policy was reviewed and by whom | October 2023 Computing Working Party |
| Date of next review and by whom | November 2024 Computing Working Party |


| | Page Number |
|---|---|
| Aims, scope and principles | 2 |
| Table of Contents | 3-4 |
| What is this Policy? | 5 |
| Who is in charge of Online Safety? | 5 |
| What are the main Online safety Risks today? | 5 |
| How Will this policy be communicated? | 5 |
| Roles and Responsibilities – Executive Headteacher and Heads of School | 6 |
| Roles and Responsibilities – Designated Safeguarding Lead /Online Safety Lead | 7 |
| Roles and Responsibilities - Governing Body, led by online safety governor | 8 |
| Roles and Responsibilities – All Staff | 9 |
| Roles and Responsibilities -PSHE/RSHE Leads | 10 |
| Roles and Responsibilities – Computing Leads | 10 |
| Roles and Responsibilities - Network Manager/technician | 10 |
| Roles and Responsibilities -Data Protection Officer | 11 |
| Roles and Responsibilities -Volunteers and contractors | 12 |
| Roles and Responsibilities - Children | 12 |
| Roles and Responsibilities -Parents/carers | 12 |
| Education and curriculum | 13 |
| Parental involvement | 13 |
| Handling online-safety concerns and incidents | 13-14 |
| Bullying | 14 |

| | |
|---|---|
| Sexual violence and harassment | 15 |
| Misuse of school technology (devices, systems, networks or platforms) | 15 |
| Social media incidents | 15 |
| Data protection and data security | 15 |
| Appropriate filtering and monitoring | 16-17 |
| Electronic communications | 17 |
| Email | 17-18 |
| School website | 19 |
| Cloud platforms | 19-20 |
| Google Workspace for Education and Seesaw platforms | 20 |
| Digital images and video | 20-21 |
| Social media-Hove Learning Federation's Social Media presence | 21-22 |
| Staff, children' and parents' Social Media presence | 22-23 |
| Device usage | 23-24 |
| Network / internet access on school devices | 24 |
| Trips / events away from school | 24 |
| Searching and Confiscating | 24-25 |
| Appendixes contents | 26 |
| Appendix 1 -Useful Online Publication Links | 27 |
| Appendix 2- Appendices Online safety (from keeping Children Safe in Education) | 27-28 |
| Appendix 3 – Online Links for Parents and Staff | 29 |
| Appendix 4 - Responding to Incident's Flow Chart | 30 |
| Appendix 5 - Teaching Staff Acceptable Use Policy | 31-33 |
| Appendix 6 – Other Staff and Volunteers / Community Users Acceptable Use Policy | 34-36 |
| Appendix 7 – Parent/Carer Acceptable Use Policy | 37 |
| Appendix 8 – Photographs and Video Consent Form | 38-39 |
| Appendix 9 – Child/ Pupil Acceptable Use Policy | 40 |

**What is this Policy?**

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 202 (KCSIE), 'Teaching Online Safety in Schools' 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside our school's statutory Safeguarding Policy. Any issues and concerns with online safety **must** follow the school's safeguarding and child protection procedures.

**Who is in charge of Online Safety?**

KCSIE makes it clear that "the designated safeguarding lead (DSL) should take lead responsibility for safeguarding and child protection (including online safety)." The Computing Subject Lead works alongside the DSL in promoting and ensuring online safety in school.

**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"). These three areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

Many of these new risks are mentioned in KCSIE 2023, e.g. fake news or upskirting.

**How will the policy be communicated?**

This policy can only impact upon practice if it is a (regularly updated) living document. It will be accessible to and understood by all stakeholders. It 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
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, Governors, children and parents/carers
- AUPs 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 may include input from staff, children and other stakeholders, helping to ensure further engagement

**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, children, 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.

**Executive Headteacher (Madeleine Southern) and Heads of School (Lorna Cummings and Ben Massey)**

## 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 Partnerships.
- 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, DPM, 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 school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles.
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of children, including risk of children being radicalized.
- 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 school's arrangements for Online Safety.
- Ensure the school website meets statutory requirements.

## Designated Safeguarding Leads / Online Safety Leads – Ben Patterson, Charlotte Wallace and Amanda Stewart

**Key Responsibilities**

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community 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" (updated July 2022)
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- Work with the Headteacher, Data Protection Manager 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.
- Stay up to date with the latest trends in online safety.
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) 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/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends.
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents.
- Liaise with school technical, pastoral, and support staff as appropriate.
- Communicate regularly with SLT and the designated safeguarding and online safety Governor/committee to discuss current issues, review incident logs.
- 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 (is it physical or technical?) and ensure staff are aware.
- Ensure the 2017 (updated 2021) DfE 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 (this now is included in Keeping Children Safe in Education 2023 pages 105-136).
- Facilitate training and advice for all staff:
    1. All staff must read KCSIE Part 1 and all those working with children
    2. It would also be advisable for all staff to be aware of Annex C (online safety)
    3. Cascade knowledge of risks and opportunities throughout the organization

**Governing Body, led by Online Safety / Safeguarding Link Governor – Lisa Marshall**

**Key responsibilities** (quotes are taken from Keeping Children Safe in Education 2023):

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board (updated October 2023)

- "Ensure an appropriate **senior member** of staff, from the school or college leadership team, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…"

- Support the school in encouraging parents and the wider community to become engaged in online safety activities

- Have regular strategic reviews with the online-safety co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at Governor meetings

- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is a 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 (Data protection Officer, Data protection manager, Designated Safeguarding Lead 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

- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A

- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated in line with advice

from the local authority and other relevant agencies, integrated, aligned and considered as part of the overarching safeguarding approach."

- "Ensure appropriate filters and appropriate monitoring systems are in place but be careful that 'over-blocking' 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. Consider a whole school approach to online safety with a clear policy on the use of mobile technology." NB – refer to 'Teaching Online Safety in Schools 2019' and investigate/adopt the UKCIS cross-curricular framework 'Education for a Connected World ' to support a whole-school approach

## 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 Leads (DSL) and Online Safety Leads (OSL) are – Ben Patterson, Amanda Stewart and Charlotte Wallace.
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education.
- Read and follow this policy in conjunction with the school's main safeguarding policy.
- Record online-safety incidents (using CPOMS) 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 policy and code of conduct/handbook.
- 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 children.
- 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 child/children are doing and consider potential dangers and the age appropriateness of websites.
- To carefully supervise and guide children 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 sources and resources before using within the classroom, including the viewing of any video footage.
- Encourage child/children to follow their acceptable use policy, remind them about it and enforce school 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 – you may find it useful to read at least the headline statistics and conclusions from the Ofcom Media Use and attitudes report 2022.
- Model safe, responsible and professional behaviours in their 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. More guidance on this point can be found in this Online Reputation Guidance

## PSHE / RSHE Lead/s – Caroline Kemp-Harris, Catrin Pierce and Rachel Dawson

**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 children' 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 children 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.

**<u>Computing Leads</u> – Ben Massey, Hannah Cutler Kathy Bruce and Matt Harper-Duffy**

**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.
- 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 school to ensure a common and consistent approach, in line with acceptable-use agreements.
- Work with the Executive Headteacher to ensure the school website meets statutory DfE requirements. See School Website Guidance

**<u>Network Manager/Technician</u> – Kevin Astle, Rab Atmani and John Nicholson**

**Key responsibilities:**

- As listed in the 'all staff' section, plus:
- Keep up to date with the school'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 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 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.

**<u>Data Protection Officer</u> – James England**

## Key responsibilities

NB – this document is not for general data-protection guidance

- Be aware of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (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 schools, 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 schools 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."*

- 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) if using any school related technology.
- 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.

## Children

## Key responsibilities

- 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 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 school'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 school staff, volunteers, Governors, contractors, children 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):

- 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 children).

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc.) in school or setting as homework/home learning tasks, all staff should encourage sensible use, monitor what child/children are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide children 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. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

## Parental involvement

- Parents' attention will be drawn to the Online Safety page for West Hove Infant School on the school website and the Online Safety page on the Hove Junior School website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This may include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

## 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/RSHE and Citizenship).

General concerns must be handled in the same way as any other safeguarding concerns.

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).

School 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 school 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 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 children 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 DSL / OSL 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 it will be referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline. – see posters.lgfl.net and reporting.lgfl.net).

The school 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 children 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).

## 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.

Also see the School Anti-Bullying Policy.

It is important **not** to treat online bullying separately to offline bullying and to recognise that much bullying will often have both online and offline elements.

## 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. 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 schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are

treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

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

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

These are defined in the relevant 'Acceptable Use Policy' as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology.

Where children 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/handbook.

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

## Social Media Incidents

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

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

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, West Hove Infant 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

"**GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe.**" Lawful and secure information sharing between schools, 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 schools 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 children, staff, Governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements.

The following data security products are used to protect the integrity of data, which in turn supports data protection:

- Sophos Anti-Virus
- Remote Access provided by Brighton & Hove City Council
- Office365 – OneDrive secure cloud storage
- Egress Encrypted email
- Send IT
- CPOMS

The Executive Headteacher, Data Protection Officer, DPO 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 Data Protection Manger and DSL should be informed in advance.

## Appropriate filtering and monitoring

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

There are two levels of filtering in place. One for children and unauthorised staff or visitors and a more relaxed set of filtering rules for approved staff. The school has the ability to maintain the block and allow lists for children.

At this school, the internet connection is provided by Brighton & Hove City Council ICT Schools & Traded Services. This means we have a dedicated and secure connection that is protected with firewalls and multiple layers of security, including a web filtering system called Smoothwall, which is designed specifically to protect children in schools. You can read more about why this system is appropriate on the UK Safer Internet Centre's appropriate filtering submission pages here.

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

At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. As the children progress through the Federation into KS2, this broadens to allow for independent but supervised Internet use.

As well as children being physically monitored, all users of the internet in school will be monitored via the Smoothwall filtering system and their browsing habits logged for reference if needed. the Head Teacher, Heads of School and Inclusion Managers receive instant, daily and weekly email notifications if any user across all sites searches for swear words or tries to access high risk categories, such as porn, violence or drugs. They can then identify who has input the search term, communicate with relevant adults and decide as a team on appropriate support and next steps.

## Electronic communications

Please read this section alongside references to pupil-staff communications in the overall school 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

- Any emails sent by children in KS1 will be from a class account that is monitored by the class teacher. Children in KS1 do not have individual email addresses.
- For KS2, pupils do have email addresses. These are solely for the purpose of accessing their Google Workspace for Education accounts. The ability to send and receive emails is disabled, unless these are enabled by a technician for the purposes of teaching a specific Computing unit.
- Children must immediately tell a teacher if they view an offensive or upsetting e-mail whilst at school.

- Staff use Office365 system or School Ping for all school emails.

Both these systems are fully auditable, trackable and managed by BHCC (Office365) and the Network Manager on behalf of the school. This is for the mutual protection and privacy of all staff, children and parents, as well as to support data protection.

General principles for email use are as follows:

- Email or School Ping is the only means of electronic communication to be used between staff and school and parents (see communication policy). Use of a different platform must be approved in advance by the data-protection manager/Executive Headteacher in advance. School Ping is also used to communicate with parents (see communication policy). Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Executive Headteacher/DPM (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.
  1. If data needs to be shared with external agencies, encrypted email via Office365 and Egress [must] be used.
  2. Internally, staff should use the school network, OneDrive or Google Drive including when working from home. Remote access may also be available for a few key members of staff, such as the Business Manager or Executive Headteacher.

- 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.

- 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 Executive Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website to various key members of staff.

The DfE has determined information which must be available on a school website. The school has completed an audit on the website to ensure that are requirements are met.

Where other 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. If in doubt, check with the School Business Manager.
- 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 schools are recognising the benefits of cloud computing platforms, not just for cost savings but to enhance teaching and learning.

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

As more and more systems move to the cloud, it becomes easier to share and access data. It is important to consider data protection before adopting a cloud platform or service – see our Data Protection policy.

For online safety, basic rules of good password hygiene should apply ("Treat your password like your toothbrush –never share it with anyone!"), expert administration and training can help to keep staff and children safe, and to avoid incidents. The Data Protection Manager analyses 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 Data Protection Manager 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 if necessary.

- Regular training ensures that all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake.

- Children and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen.

- Pupil images/videos are only made public with parental permission.

- Only school-approved platforms are used by children or staff to store pupil work.

## Google Workspace for Education and Seesaw platforms

Permission will be sought from parents for the school to create an account for their child to access the Seesaw platform in the infant school and the Google Workspace for Education in KS2. The Seesaw platform is used solely for home learning. The Google Workspace is used for home learning and to support learning within school.

The use of the Google Workspace for Education allows pupils to access a range of resources including Slides, Sheets and Docs. The pupil Google accounts have had emails disabled for pupils with any communications taking place either as private comments to class teachers or as messages in the Google Classroom stream (when this is enabled).

The school has access to all pupil accounts (with usernames and passwords kept securely) and can suspend accounts if a pupil's behavior is deemed unacceptable. Pupils are expected to follow the school's standards for behavior within the online platforms.

## Digital images and video

When a pupil joins the Federation, 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 display in children's books whilst working individually or in groups of two or more
- For display in access controlled areas of the school (such as corridors, classrooms)
- For display in an individual's leaving card

- For display in public areas of the school (such as reception, playgrounds)
- For use in the school newsletter and other printed documents (such as the prospectus)
- For use on the school website
- For use on social media (such as PTA Facebook page)
- School photographs can be provided to the media for publication or broadcast
- Class Photograph
- To give to the catering team if your child has an allergy

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

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

All staff are governed by their contract of employment, the staff handbook and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of children.

At Hove Learning Federation, no member of staff will ever use their personal phone to capture photos or videos of children, without explicit permission from the Headteacher.

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

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

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

Children 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.

Children 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.

Children 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

**Hove Learning Federation's Social Media presence**

Hove Learning Federation does not have any official social media accounts.
The Parent teacher associations at both sites have a closed Facebook page to publicise their work and events. Any Parent teacher association accounts are expected to be created in line with our school acceptable use policy for volunteers and parents.

## Staff, Children' and Parents' Social Media presence

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and children 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, children and parents, also undermining staff morale and the reputation of the school (which is important for the children we serve).

Many social media platforms have a minimum age of 13, but the school regularly deals with issues arising on social media with children 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.

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 children 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 school the next day). You may wish to introduce the Children's Commission Digital 5 A Day.

School Ping and email are the official electronic communication channels between parents and the school.

Children 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.

Children 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 children accounts.

** 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 or bring the school into disrepute. Staff are almost reminded to not state their school name on their social media pages.

## 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, and social media, misuse of technology, and digital images and video.

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

- For safety purposes while walking home without an adult, pupils in years 5 and 6 may bring a mobile phone to school, with permission from a parent or carer. These devices are handed in to the class teacher at the beginning of the school day and are then redistributed at the end of the school day. Hove Learning Federation takes no responsibility for devices that are brought into school.

- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the Digital

images and video section and Data protection and data security section, of this policy. 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 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 from the Executive Headteacher should be sought (the Executive Headteacher may choose to delegate this) and this should be done in the presence of a member staff.

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

## Network / internet access on school devices

- **Children** are not allowed networked file access via personal devices. However, they are allowed to access the school Wi-Fi network for school-related internet use using school owned devices such as iPads and Google Chromebooks. All such use is monitored.

- **Staff and trainee teachers** are not allowed networked file access via personal devices or Wi-Fi access without the permission of the Executive Headteacher. All such use is monitored.

- **Volunteers, contractors, Governors** have no access to the school network or wireless internet on personal devices without the permission of the Executive Headteacher. All such use is monitored.

- **Parents** have no access to the school network or wireless internet on personal devices, but will be provided a limited supply teacher account, if they are volunteering in school.

## Trips / events away from school

For school trips/events away from school, teachers will always have a mobile phone available to use in an emergency. If an emergency occurs the teacher will contact the school who will then liaise and contact parents if necessary. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or children 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/Principal and staff authorised by them have a statutory power to search children/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.

# Appendixes

Appendix 1 – Useful Publication Links
Appendix 2 – Excerpt from Keeping Children Safe in Education
Appendix 3 – Online links for parents and staff
Appendix 4 – Responding to Incident's Flow Chart
Appendix 5 – Teaching Staff Acceptable Use Policy
Appendix 6 – Other Staff and Volunteers / Community Users Acceptable Use Policy
Appendix 7 – Parent/Carer Acceptable Use Policy
Appendix 8 – Photographs and Video Consent Form
Appendix 9 – Child/Pupil Acceptable Use Policy

# Appendix 1 – Useful Publication Links

1. Child Protection and Safeguarding Policy
2. Positive Relationships Policy
3. Photo Consent form (Infant specific)
4. Online-Safety Questions from the Governing Board (UKCIS)
5. Education for a Connected World cross-curricular digital resilience framework (UKCIS)
6. Working together to safeguard children (DfE)
7. Searching, screening and confiscation advice (DfE)
8. Sexting guidance from UKCIS
    - Overview for all staff
    - Full guidance for school DSLs
10. Prevent Duty Guidance for Schools (DfE and Home Office documents)
11. Data protection and data security advice
12. Preventing and tackling bullying (DfE)
13. Online bullying: advice for Headteachers and school staff (DfE)

# Appendix 2 – Excerpt from Keeping Children Safe in Education

## Annex C: Online safety **(from Keeping Children Safe in Education 2023)**

135. It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

136. The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk: content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism. contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes. conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

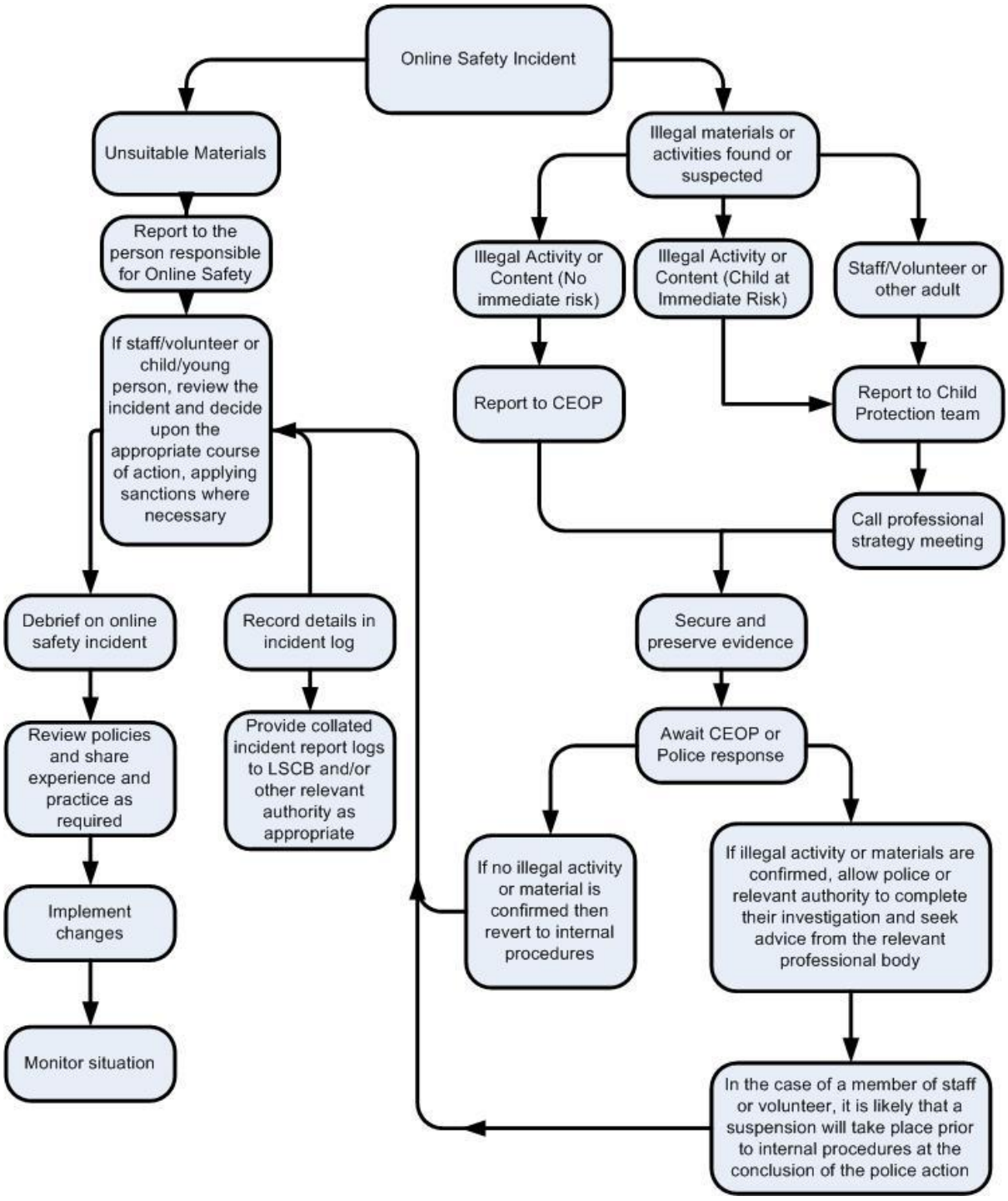
137. Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.

# Appendix 3 - Online links for parents and staff

| Organisation/Resource | What it does/provides |
|---|---|
| thinkuknow | NCA CEOPs advice on online safety |
| Disrespect Nobody | Home Office advice on healthy relationships, including sexting and pornography |
| UK Safer Internet Centre | Contains a specialist helpline for UK colleges and schools |
| SWGfL | Includes a template for setting out Online Safety Policies |
| Internet Matters | Help for parents on how to keep their children safe online |
| Parent Zone | Help for parents on how to keep their children safe online |
| Childnet Cyberbullying | Guidance for schools on cyberbullying |
| PSHE Association | Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images |
| Educate Against Hate | Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation |
| The use of social media for online radicalisation | A briefing note for schools on how social media is used to encourage travel to Syria and Iraq |
| UKCIS | The UK Council for Internet Safety's Website provides:<br>● Sexting Advice<br>● Online Safety – Questions for Governing Bodies<br>● Education for a connected world framework |
| | |
| NSPCC | NSPCC advice for schools and colleges |
| Net Aware | NSPCC advice for parents |
| Common Sense Media | Independent reviews, age ratings and other information about all types of media for children and their parents |
| Searching, screening and confiscation | Guidance to schools on searching children in schools and confiscating items such as mobile phones |
| LGfL | Advice and resources from the London Grid for Learning |

# Appendix 4 – Responding to Incident's Flow Chart

## Responding to incidents of misuse – flow chart



# Appendix 5 – Teaching Staff Acceptable Use Policy

Teaching Staff Acceptable Use Policy agreement

As a member of school staff I understand that I take responsibility for the following role in Online Safety:

| Statement | Notes | Initialed to say read understood and agreed. |
|---|---|---|
| I have read the Online Safety policy. | *This will be given as part of the induction pack and for other staff will be provided as part of the policy pack which is to be read each year.* | |
| I have read, understood and signed the Staff Acceptable Use Policy (AUP) | *That is this list.* | |
| I will report any suspected misuse or problem to the *Executive Head-teacher / Senior Leader; Online Safety Coordinator / ICT Technicians* for investigation / action / sanction as appropriate. | *If I know there to be an issue I will inform the relevant person.* | |
| I agree that any digital communications with children / parents / carers should be on a professional level *and* only carried out using official school systems. Any such communication will be professional in tone and manner.<br>If I am friendly with parents /carers out of school, I will remain professional in my conduct and respect all requirements for data and pupil protection.<br><br>If a child joins our school which I have a legitimate pre-existing relationship with e.g. family or close friend, I will inform the school of this relationship. Any digital communication with this child will be through the child's parents and not to the child directly.<br><br>I will not communicate with any past or present children, under the age of 16 using digital media. | *To use school email accounts to send school emails and if I have parent or carer as friends outside work I will not use my personal email etc. to talk about school issues.* | |
| Teaching staff will ensure Online Safety issues are embedded in all aspects of the curriculum and other activities. Other staff will support the teaching staff in ensuring that these activities are undertaken when directed to do so. | *I will ensure that my children are made aware of Online Safety issues and will refer to these on a regular basis.* | |
| I will ensure that children understand and follow the Online Safety and acceptable use policies. | *Tell children what acceptable use is and deal with any incident where these rules are broken.* | |
| When using internet devices I will teach children to begin to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations | *I will expect children to be able to say whether the work is their own or that of another person. As they move through the school they will be expected to begin to say where they found the information.* | |
| I will monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices | *When children in my care are using technology I will ensure they are properly supervised.* | |
| *In lessons where internet use is pre-planned children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches* | *I will use trusted sites e.g. BBC, expresso etc. where possible and if directing children to a new site I will have checked they are suitable for the children's use.* | |

| | | |
|---|---|---|
| *I will only use school cameras or equipment to take photographs, videos or audio of children. I will only load the above onto a school computer, school memory stick or school laptop* | *No use of own phones or cameras and not saved onto home computers or home devices.* | |
| *I will keep all passwords to school systems private and secure and if they are written down I will make sure they are not obvious what they are for. If I lose a list of passwords or feel others may know what they are I will change my passwords.* | *Write down passwords without writing next to them what they are for. Try to disguise passwords e.g. as a phone number or word in sentence.* | |
| *I will lock PC screens before leaving the room* | *Do not let other gain access to sensitive information* | |
| *I understand that if others access the school systems using my own personal password I personally could be liable for disciplinary action if anything malicious happens because of this access.* | *Do not let others use your login details where possible.* | |
| *If I take photographs of children, I will ensure they are suitably dressed and not partaking in activities which could bring themselves or the school into disrepute.* | *For example - PE lessons are ok but not the children changing. If a photograph is of a child doing something they could be disciplined for then it should only be taken with permission of senior leader e.g. swearing, fighting etc.* | |
| *I will not publish any pupil's photographs on a website or social media site. If publishing on the school website I will have permission from the parents for the use of photographs in this way and I will not name any children in the photographs.* | *E.g. If you go on a trip no pictures on Facebook etc. later on.* | |
| *I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.* | *The monitoring of the school system will mean that you will be found out of you are doing this.* | |
| *I know that any internet usage on school devices is monitored and therefore if I accidentally access any offensive or pornographic material I will report the incident to a senior leader.* | *If you accidentally access inappropriate material and do not inform a senior leader you may be disciplined later for non-accidental access of the material.* | |
| *I will not send personal data over the internet or taken off the school site unless safely encrypted or otherwise secured. I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Workforce Privacy Notice Paper based Protected and Restricted data must be held in lockable storage.* | *You need to save it on an encrypted memory stick, use a school laptop or use home access to access personal data whilst off the school site.* | |
| *I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.* | | |
| *I will not access, copy, remove or otherwise alter any other user's files, without their express permission.* | | |
| *I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.* | | |

| | | |
|---|---|---|
| *I will not engage in any on-line activity that may compromise my professional responsibilities.* | | |
| *I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)* | | |
| *I will not install or attempt to install programmes of any type from a non-reputable and trusted site on a machine, or store programmes on a computer. If I am not sure about the suitability of any download I will refer the matter to an ICT technician to do this for me.* | *The school system will not allow you to download and install some types of programs so need to get a technician to do this for you. If downloading other programs be aware that unless it is from a reputable site you could be opening up the school system to viruses.* | |
| *I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others.* | *Any damage caused must be reported and any malicious damage may lead to disciplinary action.* | |
| *I will ensure that I have permission to use the original work of others in my own work* | | |
| *Where work is protected by copyright, I will not download or distribute copies (including music and videos).* | *Making copies of items you would usually pay for and giving it to somebody else to use or own is illegal. E.g. burning a copy of a CD or DVD you have brought and giving to a friend. Copying software discs to home computers is not covered by our site licenses.* | |
| *I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.* | *Some breaches of this policy can result in further action being taken. See the Online Safety policy for more details.* | |

# Appendix 6 – Other Staff and Volunteers / Community Users Acceptable Use Policy

## Staff and Volunteers Acceptable Use Policy

**This Acceptable Use Policy is intended to ensure:**

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *children / children's* learning and will, in return, expect staff and volunteers to agree to be responsible users.

## Acceptable Use Policy Agreement

| Statements | Notes | |
|---|---|---|
| I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. | Not opening suspicious email attachments. Not sharing passwords, keeping virus protection up to date etc. | |
| I recognise the value of the use of ICT for enhancing learning and will ensure that children receive opportunities to gain from the use of ICT. | | |
| I will, where possible, educate the young people in my care in the safe use of ICT and embed Online Safety in my work with young people. | | |
| I understand that the school will monitor my use of the ICT systems, email and other digital communications. | | |
| I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school | | |
| I understand that the school ICT equipment are primarily intended for educational use and that I am personally responsible for the non-educational use of any school provided equipment. | | |
| I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it. | | |
| I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person. | | |
| I will not access, copy, remove or otherwise alter any other user's files, without their express permission. | | |

| | | |
|---|---|---|
| I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions. | | |
| I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured. | | |
| I will only use chat and social networking sites in school in accordance with the school's policies. | | |
| I will only communicate with children and parents / carers using official school systems. Any such communication will be professional in tone and manner. (schools should amend this section to take account of their policy on communications with children and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications) | | |
| I will not engage in any on-line activity that may compromise my professional responsibilities. | | |
| When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses. | | |
| I will not use personal email addresses on the school ICT systems. | | |
| I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes) | | |
| I will ensure that my data is regularly backed up, in accordance with relevant school / academy policies. | | |
| I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials. | | |
| I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work. | | |

| | | |
|---|---|---|
| I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies. | | |
| I will not disable or cause any damage to school equipment, or the equipment belonging to others. | | |
| I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage. | | |
| I understand that data protection policy requires that any staff or children / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority. | | |
| I will immediately report any damage or faults involving equipment or software, however this may have happened. | | |
| I will ensure that I have permission to use the original work of others in my own work | | |
| Where work is protected by copyright, I will not download or distribute copies (including music and videos). | | |
| I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school / academy | | |
| I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include; a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police. | | |

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

# Appendix 7 – Parent/Carer Acceptable Use Policy

## Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

### This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of Online Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that children will have good access to digital technologies to enhance their learning and will, in return, expect the children to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

## Permission Form

Parent / Carers Name | | Children / Pupil Name | |

As the parent / carer of the above *child / children*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

*I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, Online Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.*

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's Online Safety.

I will be aware that some website, social media, games and Apps have legal age limits. When my child is in my care I will only allow my child access to appropriate content for their age and maturity.

Signed | | Date | |

# Appendix 8– Photographs and Video Consent Form

## Photographs and Video Consent Form

Photographs and videos will be used where they are deemed essential for performing the public task of the school. Where photographs are required for other purposes, these purposes will be documented and explicit consent sought.

The retention period for photographs and videos will be documented in the retention policy. At the end of the retention period photographs will either be destroyed, or may be retained photos for archiving purposes in the public interest.

Please also note that when your child is in a public venue (such as a county sports event) local media may take photos. You are able to object to this processing and we will give you prior knowledge if and when we know third-parties will be present at external events.

Where photographs are used as part of a display we will not accompany the photograph with any other identifiable information such as names.

Photographs and video will only be taken using school equipment and must represent the school and children positively – inappropriate, negative, embarrassing or distressful photos will not be used.

Consent will be sought from parents/careers. Where parental consent has been obtained, this will be use as the lawful basis.

We collect and use photographs for the following purposes.

Please tick the box to confirm you agree to the use of photographs for that purpose:

| | |
|---|---|
| For display in children's books whilst working individually or in groups of two or more | |
| For display in access controlled areas of the school (such as corridors, classrooms) | |
| For display in an individual's leaving card | |
| For display in public areas of the school (such as reception, playgrounds) | |
| For use in the school newsletter and other printed documents (such as the prospectus) | |
| For use on the school website | |
| For use on social media (such as PTA Facebook page) | |
| School photographs can be provided to the media for publication or broadcast | |

### Note:

Photographs used in YR for each child's individual learning diary will be explained by your child's class teacher and consent will be sought at this point.

### I have read and understood the information.

I agree for my / my child's photographs and video to be used for the purposes described.

| | |
|---|---|
| Pupil Name | |
| Name of parent/carer | |
| Signature of parent/carer | |
| Date: | |

If you wish to withdraw consent, please ask the school office for a consent withdrawal form

# Appendix 9 – Child/Pupil Acceptable Use Policy

## My Computing Rules

**At Hove Learning Federation the children learn some simple rules for keeping themselves safe when using the computer. Please read and agree the rules below with your child:-**

If I am writing a message (postie, blog, or other message) or anything that someone else will read (e.g. a home page or wiki).

I will:

- always ask a grown up before I use a computer;
- only send an online message if a grown up knows;
- be kind and polite – do not hurt anyone's feelings;
- never log on as someone else;
- only use a nickname or first name;
- never share my address;
- never talk to strangers;
- be clear – write in sentences;
- be polite – SHOUTING is rude!

If I am reading a message or looking at anything on the computer.

I will: tell a grown up I trust if I don't like something I see or it upsets me

If you understand these rules please put a tick in the box below and ask your parents or carers to the sign the form.

**Child's name**……..……

**Parent/Carers name**……

**Date**…….……