L.E.A.D. Academy Trust
Lead • Empower • Achieve • Drive

# L.E.A.D. ACADEMY TRUST

# Online Safety Policy

## Policy/Procedure management log

| | |
|---|---|
| **Document name** | Online Safety Policy |
| **Author** | Lee Jepson/Rebecca Hyder/Helen Tunney |
| **Date approved** | December 2023 |
| **Date issued** | **November 2023** |
| **Date of review** | **November 2024** |

# Contents

# Introduction – L.E.A.D.

L.E.A.D. Academy Trust fully recognises its moral and statutory responsibility to safeguard and promote the welfare of all pupils. The Trust endeavours to provide a safe and welcoming environment in all its academies, where children are respected and valued.

Section 157 of the Education Act 2002 and the Education (Independent Schools Standards) (England) Regulations 2003 require proprietors of independent schools (including academies and city technology colleges) to have arrangements to safeguard and promote the welfare of children. In line with this requirement,

**Aims**

- To ensure that all practices of each academy and its stakeholders contribute towards the safeguarding and promoting of the welfare of all young people – pupils' welfare is of paramount importance.
- To emphasise how online safety is part of safeguarding and promoting the welfare of all young people and is the primary responsibility of all staff, governors, and volunteers.
- To outline the safe working practices that all staff, governors, and volunteers should undertake when working with young people.
- To communicate clear procedures for identifying, reporting, and recording suspected cases of abuse, extremism, and radicalisation.
- To support the mission, vision and values of the Trust and its member academies.

## Who is responsible for the policy?

- The Trust has overall responsibility for the development and effective operation of this policy. The Trust has delegated day-to-day responsibility for operating the policy to each individual Trust academy, the academy governing body (AGB) and the Headteacher.
- The AGB and senior leadership team at each Trust academy have specific responsibilities to ensure the fair application of this policy and all are responsible for supporting colleagues and ensuring its success.
- This policy must be implemented alongside the procedural guidance set out by the local authority in which the academy is located.

## The Trust's commitment

- Everyone who comes into contact with children and their families has a role to play in safeguarding children. Academy staff are particularly important as they are in a position to identify concerns early and provide help for children, and to prevent concerns from escalating.
- The Trust is committed to providing safe, caring, and welcoming environments where every child is able to reach their full potential free from harm, abuse, and discrimination. All staff and volunteers are expected to discharge their safeguarding responsibilities, including online safety, effectively and recognise that high self-esteem, confidence, peer support and clear lines of communication with trusted adults helps all children, especially those at risk of or suffering abuse, to thrive.
- All academies will be alert to the signs of abuse, neglect and radicalisation and follow procedures to ensure that children receive effective support, protection, and justice.

- Academies will work with social care, the police, health services and other services (such as Channel co-ordinators/police practitioners where appropriate) to promote the welfare of children and protect them from harm.

## Online Safety Policy - Scope

This Online Safety Policy outlines the commitment of the Birley Academy to safeguard members of our school community online in accordance with statutory guidance and best practice.

**This Online Safety Policy applies to all members of the academy community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of academy digital systems, both in and out of our academy. It also applies to the use of personal digital technology on the academy site (where allowed).**

The Birley Academy will deal with such incidents within this policy and associated behaviour, safeguarding and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of our academy.

## Policy development, monitoring and review

This Online Safety Policy has been developed by the Online Safeguarding Group made up of:

- Designated safeguarding lead (DSL)
- Online Safety Lead (OSL)
- staff – including teachers/support staff/technical staff.
- governors
- parents and carers
- community users

Consultation with the whole academy community has taken place through a range of formal and informal meetings.

## Schedule for development, monitoring and review

| | |
|---|---|
| This Online Safety Policy was approved by the *academy governing body on:* | *5 December 2023* |
| The implementation of this Online Safety Policy will be monitored by: | *Miss T. Shelley (DSL) –* ***Updated April 2024*** |
| Monitoring will take place at regular intervals: | *Half-termly* |
| The *governing body* will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals: | *At each AGB as part of the headteachers report to governors* |
| The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | *December 2024* |
| Should serious online safety incidents take place, the following external persons/agencies should be informed: | *The Sheffield Childrens' Safeguarding Partnership - (0114) 2734855*<br><br>*South Yorkshire Police, Moss Way, Sheffield, S20* |

## Process for monitoring the impact of the Online Safety Policy

The academy will monitor the impact of the policy using:

- logs of reported incidents
- Filtering and monitoring logs
- internal monitoring data for network activity
- surveys/questionnaires of:
  - learners
  - parents and carers
  - staff.

## Policy and leadership

## Responsibilities

To ensure the online safeguarding of our academy community it is important that all members work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the academy.

### Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of our academy and fostering a culture of safeguarding. Though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and (at least) another member of the senior leadership team will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, L.E.A.D I.T Services and their technical staff and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in the academy who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and L.E.A.D I.T. Services in all aspects of filtering and monitoring.

### Governors

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

*"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety".*

*"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"*

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".

This review will be carried out by a sub-group of the AGB whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

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

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

### Designated Safety Lead (DSL)

*Keeping Children Safe in Education states that:*

*"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."*

*They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college".*

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

While the responsibility for online safety is held by the DSL and cannot be delegated, the school also has an Online Safety Lead who works to support the DSL in carrying out these responsibilities. It is recommended that the school reviews the sections below for the DSL and OSL and allocate roles depending on the structure it has chosen.

### The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.

- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out.
- attend relevant governing body meetings/groups.
- report regularly to headteacher/senior leadership team.
- be responsible for receiving reports of online safety incidents, handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety).

### Online Safety Lead

The Online Safety Lead will:

- lead the Online Safety Group (DSL; AHT for PD; IT Lead Technician; parents/carers; student Ambassadors).
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments.
- have a leading role in establishing and reviewing the academy's online safety policies and related statements.
- promote an awareness of and commitment to online safety education / awareness raising across the academy and beyond.
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners.
- liaise with (academy / local authority / Trust and teaching school / external providers) technical staff, pastoral staff and support staff (as relevant).
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

### Curriculum Leads

Curriculum Leads will work with the DSL and OSL to develop a planned and coordinated online safety education programme e.g., Project EVOLVE .

This will be provided through:

- PHSE and SRE programmes

- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

### Teaching and support staff

Academy staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current Online Safety Policy and practices.
- they understand that online safety is a core part of safeguarding.
- they have read, understood, and signed the staff acceptable use agreement (AUA).
- they immediately report any suspected misuse or problem to the DSL for investigation/action, in line with the academy safeguarding procedures.
- all digital communications with learners and parents/carers are on a professional level and only carried out using official academy systems. In line with the staff Code of Conduct and Acceptable Use Agreements.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other activities (where allowed) and implement current policies regarding these devices.
- in lessons where internet use is pre-planned learners are 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.
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies (e.g. the guidance contained in the SWGfL Safe Remote Learning Resource).
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of the academy and in their use of social media.

### L.E.A.D I.T Services

The DfE Filtering and Monitoring Standards says:

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

*"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet*

*the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."*

*"*L.E.A.D. I.T Services have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems".

"L.E.A.D. I.T Services will work with the senior leadership team and DSL to:

- procure systems.
- identify risk.
- carry out reviews.
- carry out checks.

"We are aware that there may not be full-time staff for each of these roles, and responsibility may lie as part of a wider role within the academies. However, it must be clear who is responsible, and it must be possible to make prompt changes to your provision."

As we at the Birley Academy have a technology service provided by L.E.A.D. I.T Services, it is our responsibility to ensure that L.E.A.D. I.T Services carries out all the online safety measures that the academy's obligations and responsibilities require. It is also important that L.E.A.D. I.T Services follows and implements our Online Safety Policy and procedures.

L.E.A.D. I.T Services is responsible for ensuring that:

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

### Learners

- are responsible for using the academy digital technology systems in accordance with our learner acceptable use agreements and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies out of the academy and realise that the academy's Online Safety Policy covers their actions out of the academy, if related to their membership of the academy.

### Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

At the Birley Academy we will take every opportunity to help parents and carers understand these issues through:

- publishing the academy Online Safety Policy on our website
- publish information about appropriate use of social media relating to posts concerning the academy.
- seeking their permissions concerning digital images, cloud services etc (see parent/carer AUA in the appendix)
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the academy in:

- reinforcing the online safety messages provided to learners.

### Community users

Community users who access the academy Internet as part of the wider academy provision will be expected to agree to the AUG, via a link to the academy website.

### Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the academy community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. Depending on the size or structure of the academy this group may be part of the safeguarding group. The group will also be responsible for regular reporting to senior leaders and the governing body.

The Online Safety Group may have the following members:

- Designated Safeguarding Lead
- online safety lead
- senior leaders
- technical staff

- teacher and support staff members
- learners
- parents/carers

Members of the Online Safety Group will assist the DSL/OSL with:

- the production/review/monitoring of our academy Online Safety Policy/documents
- the production/review/monitoring of our filtering procedures and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage.
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of learners to staff awareness, emerging trends and our online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision.
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

The Online Safety Group terms of reference can be found in the appendices to this policy.

## Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of academy life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of our academy and wider community, using officially sanctioned mechanisms.

## Policy

## Online Safety Policy

The Birley Academy's Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication.
- allocates responsibilities for the delivery of the policy.
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours.
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the academy, and how they should use this understanding to help safeguard learners in the digital world.
- describes how we will help prepare learners to be safe and responsible users of online technologies.
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms.
- is supplemented by a series of related acceptable use agreements.
- is made available to staff at induction and through normal communication channels, including staff training, on-line training, whole staff briefings.
- is published on our academy website.

## Acceptable use.

### Acceptable use agreements

Our Acceptable Use Agreement is a document that outlines Birley Academy's expectations on the responsible use of technology by its users. They are signed or acknowledged by staff as part of their conditions of employment. We also require learners and parents/carers to sign them, though it is more important for these to be regularly promoted, understood and followed rather than just signed. There is a range of acceptable use agreements in the appendices along with a table of actions.

The Birley Academy Online Safety Policy and acceptable use agreements define acceptable use. The acceptable use agreements will be communicated/re-enforced through:

- staff induction and handbook.
- splash screens.
- digital signage.
- posters/notices around where technology is used.
- communication with parents/carers.
- built into education sessions.
- academy website.
- peer support.

When using communication technologies, we at the Birley Academy considers the following as good practice:

- when communicating in a professional capacity, staff will ensure that the technologies they use are officially sanctioned by the academy.
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- Staff are be expected to follow good practice when using personal social media regarding their own professional reputation and that of the academy and its community.
- users should immediately report to a nominated person – in accordance with academy policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- relevant policies and permissions should be followed when posting information online e.g., academy website and social media. Only academy e-mail addresses should be used to identify members of staff and learners.

### Reporting and responding

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. The Ofsted review suggested:

*"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. In*

*order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:*

- *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse".*

Therefore, we at Birley Academy will take all reasonable precautions to ensure online safety for all users but recognise that incidents may occur inside and outside of our academy (with impact on the academy) which will need intervention. We will ensure:

- there are clear reporting routes which are understood and followed by all members of the academy community which are consistent with our safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of our community will be made aware of the need to report online safety issues/incidents.
- reports will be dealt with as soon as is practically possible once they are received within 24 hours of receiving as a maximum.
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident will be escalated through the agreed academy safeguarding procedures, this may include:

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

- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher or where there is a conflict of interest in reporting to the headteacher, in which case the complaint is referred to the Director of School, Trust DSL and the local authority.
- where there is no suspected illegal activity, devices may be checked using the following procedures:
- two senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- conduct the procedure using an academy owned device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.

- ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form.
- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - internal response or discipline procedures
    - involvement by local authority / Trust (as relevant)
    - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.
- There are support strategies in place e.g., peer support for those reporting or affected by an online safety incident.
- incidents should be logged on MyConcern and where appropriate Confide.
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant / necessary)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with.
    - staff, through regular briefings.
    - learners, through assemblies/lessons.
    - parents/carers, through newsletters, school social media, website.
    - governors, through regular safeguarding updates.
    - local authority/external agencies, as relevant.

*The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour".*

The academy will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

### Harmful Sexual Behaviour

At Birley Academy, we recognise that sexual violence and sexual harassment occurring online (either in isolation or in connection with face-to-face incidents) can introduce a number of complex factors. Among other things, this can include widespread abuse or harm across social media platforms that leads to repeat victimisation. Online concerns can be especially complicated, and support is available from a range of organisations – see the links section. For this reason, we ensure that we have a robust, up-to-date and comprehensive online safety policy which links to other relevant safeguarding policies.

Our academy has a zero-tolerance approach to any harmful sexual behaviour involving children and acknowledge that it could be occurring at Birley Academy and in our community. We adopt a proactive approach to assessing prevalence, responding to incidents, and challenging and changing behaviour. This statement applies to all governors, staff and learners.

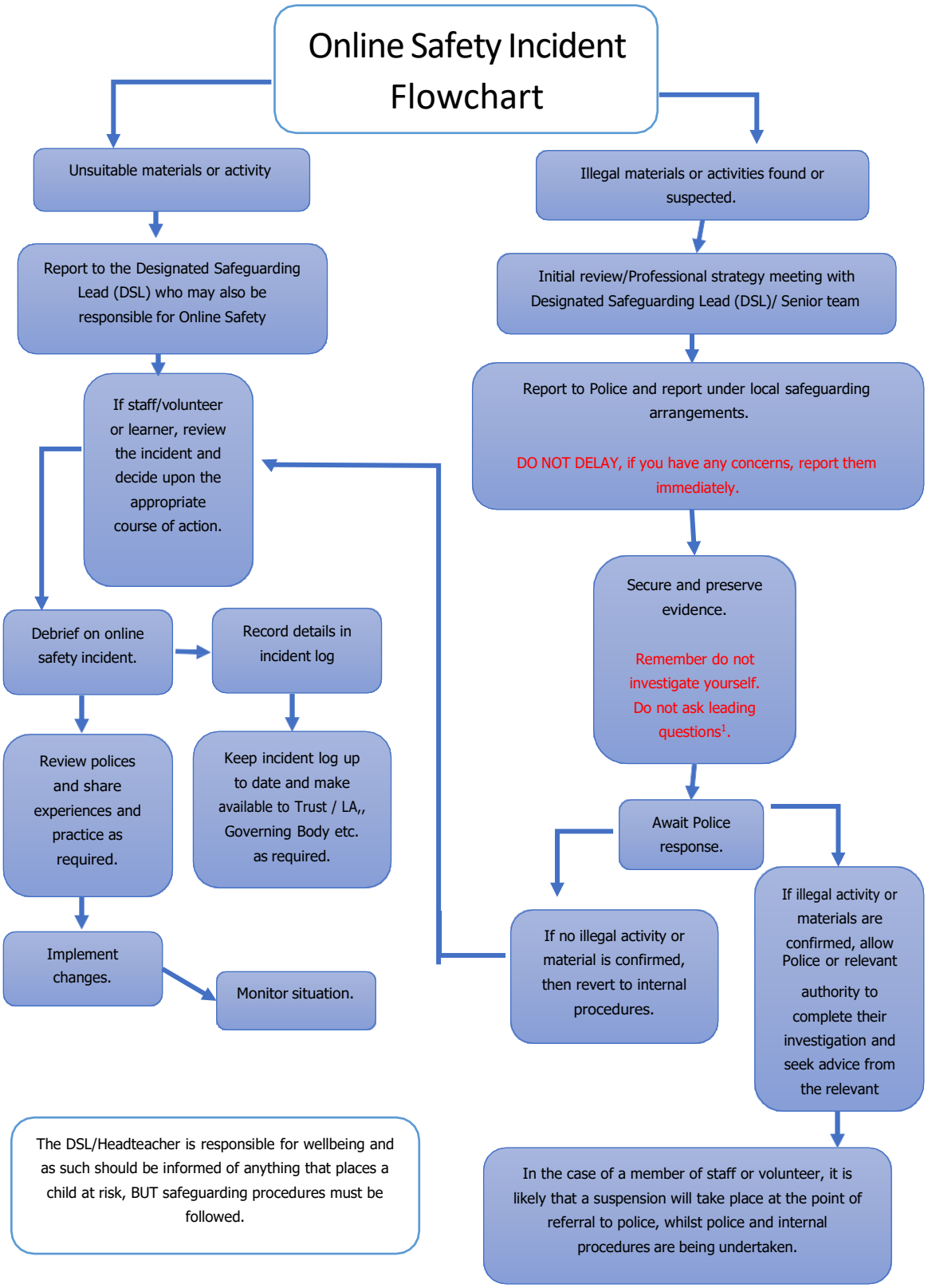
We have a statutory duty to safeguarding the children in our setting. We work together to foster an environment that creates healthy relationships for children and young people.

Our whole-school approach encourages healthy relationships and works to prevent harmful sexual behaviour. We provide high quality education within the curriculum to reduce the likelihood of the situations occurring.

We recognise that HSB is harmful to both the child/children affected by the behaviours and the child/children who displayed the behaviour and provide ongoing support for all involved.

Our approach is to treat everything as safeguarding incident in the first instance - we distinguish between behaviours that are exploratory and part of healthy age and ability appropriate development and those that may be harmful.

As an academy we provide regular opportunities for staff to understand what harmful sexual behaviours might look like and what they should do in the event of a report.


Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident.
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to Trust / LA,, Governing Body etc. as required.
Implement changes.
Monitor situation.
Illegal materials or activities found or suspected.
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Await Police response.
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

## Academy actions

It is more likely that we at Birley Academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of our community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary/safeguarding procedures.

## Responding to Learner Actions

| Incidents | Refer to class teacher/tutor | Refer to Head of Department / Principal Teacher / Deputy Head | Refer to Headteacher | Refer to Police/Social Work | Refer to L.E.A.D. I.T Services / local authority technical support for advice/action | Inform parents/carers | Remove device/ network/internet access rights | Issue a warning | Further sanction, in line with behaviour policy |
|---|---|---|---|---|---|---|---|---|---|
| Deliberately accessing or trying to access material that could be considered illegal (see list on unsuitable/inappropriate activities in appendices). | | X | X | X | X | X | X | | X |
| Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords | X | X | | | X | | | X | X |
| Corrupting or destroying the data of other users. | X | X | | | X | | | | X |
| Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | X | | | X | | | X |
| Unauthorised downloading or uploading of files or use of file sharing. | X | X | | | X | | | X | X |
| Using proxy sites or other means to subvert the school's filtering system. | | X | | | X | | | | X |
| Accidentally accessing offensive or pornographic material and failing to report the incident. | | X | X | | X | X | X | | X |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Deliberately accessing or trying to access offensive or pornographic material. | | X | X | X | X | X | X | | X |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act. | | X | | | X | | | | X |
| Unauthorised use of digital devices (including taking images) | | X | X | | X | X | X | | X |
| Unauthorised use of online services | X | X | | | X | | | | X |
| Actions which could bring the school into disrepute or breach the integrity or the ethos of the school. | X | X | X | | X | X | | X | X |
| Continued infringements of the above, following previous warnings or sanctions. | | | X | | X | X | | | X |

## Searching Screening and Confiscating

Members of staff will be made aware of the academy's statement on "Electronic devices – searching, confiscation and deletion", held within the academy Behaviour Policy:

- at induction
- at regular updating sessions on the academy's online safety / safeguarding / behaviour management policy
- in safeguarding training and briefings

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data/files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

The Headteacher will publicise the academy's behaviour policy, in writing, to staff, parents/carers and learners at least once a year.

## Responding to Staff Actions

| Incidents | Refer to line manager | Refer to Headteacher/ Principal | Refer to local authority/MAT/HR | Refer to Police | Refer to LA / Technical Support Staff for action re filtering, etc. | Issue a warning | Suspension | Disciplinary action |
|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)** | | X | X | X | X | | X | X |
| Deliberate actions to breach data protection or network security rules. | | X | X | | X | | | X |
| Deliberately accessing or trying to access offensive or pornographic material | | X | X | X | X | | X | X |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | X | X | Depends on data | X | | X | X |
| Using proxy sites or other means to subvert the school's filtering system. | | X | X | Depends on data | | X | Depends on data | X |
| Unauthorised downloading or uploading of files or file sharing | | X | X | Depends on data | | X | Depends on data | X |
| Breaching copyright or licensing regulations. | | X | X | | | X | | |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, | X | X | LEAD IT | | X | X | X | If repeatedly happens and impact |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| using another person's account. | | | | | | | | |
| Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | Depending on nature | Depending on nature | X | X | Possible | Possible |
| Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers | X | | | | | | | X |
| Inappropriate personal use of the digital technologies e.g. social media / personal e-mail | X | | | | | | | X |
| Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner | X | | X | | X | | | |
| Actions which could compromise the staff member's professional standing | | X | X | | X | | | X |
| Actions which could bring the school into disrepute or breach the integrity or the ethos of the school. | | X | X | | X | | | X |
| Failing to report incidents whether caused by deliberate or accidental actions | | X | X | Depending on nature | X | Depending on nature | | X |
| Continued infringements of the above, following previous warnings or sanctions. | | X | X | | X | | Depending on nature | X |

## Online Safety Education Programme

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of Birley Academy's online safety provision. Learners need the help and support of our academy to recognise and avoid online safety risks and develop their resilience.

***The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:***

*"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'."*

***Keeping Children Safe in Education states:***

*"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 …"*

Online safety will be a focus in all areas of the curriculum and staff will reinforce online safety messages. The online safety curriculum is embedded into our safeguarding curriculum maps where there is evidence of a broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected World Framework by UKCIS/DCMS and the SWGfL Project Evolve and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning.
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes.
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g., PHSE; SRE; Literacy etc.
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- Learners will be helped and supported to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the CyberChoices site.
- staff will act as good role models in their use of digital technologies the internet and mobile devices (as defined in the code of conduct)
- in lessons where internet use is pre-planned, learners will 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.
- where learners are allowed to freely search the internet, staff will be vigilant in supervising the learners and monitoring the content of the websites the young people visit.
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g., racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a

situation, staff will be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, will be recorded and auditable, with clear reasons for the need.

- the online safety education programme will be relevant and up to date to ensure the quality of learning and outcomes.

## Contribution of Learners

At Birley Academy we acknowledge, learn from, and use the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for our academy community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvass learner feedback and opinion.
- appointment of on-line safety ambassadors/anti-bullying ambassadors
- the Online Safety Group has learner representation.
- learners contribute to the online safety education programme e.g. peer education, digital leaders. leading lessons for younger learners, online safety campaigns.
- learners designing/updating acceptable use agreements.
- contributing to online safety events with the wider school community e.g., parents' evenings, family learning programmes etc.

## Staff/volunteers

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

*"All staff should receive appropriate safeguarding and child protection training (**including online safety**) at induction. The training should be **regularly updated**. In addition, all staff should receive safeguarding and child protection (**including online safety**) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."*

*"Governing bodies and proprietors should ensure... that safeguarding training for staff, **including online safety** training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning.**"***

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff, at least annually. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the academy's annual safeguarding and data protection training for all staff.

- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand our academy online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- the Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g., UKSIC / SWGfL / MAT / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- the Designated Safeguarding Lead/Online Safety Lead will provide advice/guidance/training to individuals as required.

### Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority/ trust or other relevant organisation (e.g., SWGfL)
- participation in academy level training / information sessions for staff or parents, this may include attendance at assemblies/lessons).

A higher level of training will be made available to (at least) the Online Safety Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the academy's filtering and monitoring provision, in order that they can participate in the required checks and review.

### Families

Parents and carers play an essential role in the education of their children and in the monitoring/regulation of their children's online behaviours. However, they may have a limited understanding of online safety risks and issues. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

At Birley Academy we will seek to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
- the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.
- letters, newsletters, website, learning platform,

- high profile events / campaigns e.g., safer internet day
- reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix for further links/resources).
- Sharing good practice with other schools in clusters and or LA / Trust

## Adults and Agencies

At Birley Academy we will provide opportunities for local community groups and members of the wider community to gain from the academy's online safety knowledge and experience. This may be offered through the following:

- online safety messages targeted towards families and relatives.
- providing family learning courses in use of digital technologies and online safety
- providing online safety information via their website and social media for the wider community
- supporting community groups, e.g., early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision.

## Technology

*The DfE Filtering and Monitoring Standards states that "Your IT service provider may be a staff technician or an external service provider".*

We at Birley Academy use our internal IT Support Function known as L.E.A.D. IT Services. L.E.A.D. I.T Services are our IT service provider. We are aware that it is our responsibility to ensure that they carry out all the online safety and security measures that would otherwise be the responsibility of the Academy. We ensure that L.E.A.D. I.T Services and the internal IT team are fully aware of the school Online Safety Policy/acceptable use agreements.

The academy and the internal IT Team are responsible for ensuring that the technical infrastructure/network is as safe and secure as is reasonably possible and that processes and procedures approved within this policy are implemented. We will ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection. A more detailed technical security statement can be found in the Appendices.

## Filtering & Monitoring

*The DfE guidance (for England) on filtering and monitoring in KCSIE" states:*

*"It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an*

*awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified…*

*The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards"*

Our academy filtering and monitoring provision is agreed by senior leaders, governors and L.E.A.D. I.T Services (L.E.A.D. I.T) and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and L.E.A.D. I.T Services will have technical responsibility for ensuring the filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the L.E.A.D. I.T Services.

- checks on the filtering and monitoring system are carried out by L.E.A.D. I.T Services with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g., remote access or BYOD or new technology is introduced.

## Filtering

- Birley Academy manages access to content across its systems for all users and on all devices using the academy's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective.
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes (see Appendix for more details).
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- our academy has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)
- younger learners will use child friendly/age-appropriate search engines e.g., SWGfL Swiggle
  the academy has a mobile phone statement (appendix C2) and where personal mobile devices have internet access through the academy network, content is managed in ways that are consistent with policy and practice.

- access to content through non-browser services (e.g., apps and other mobile technologies) is managed in ways that are consistent with policy and practice.

## Monitoring

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

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

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

## Technical Security

Birley Academy technical systems will be managed in ways that ensure that we meet recommended technical requirements. As a minimum:

- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- all users have clearly defined access rights to academy technical systems and devices. Details of the access rights available to groups of users will be recorded by L.E.A.D. I.T Services and will be reviewed, at least annually, by the SLT/Online Safety Group
- password policy and procedures are implemented. (consistent with guidance from the National Cyber Security Centre)
- the security of their username and password and must not allow other users to access the systems using their log on details.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- all academy networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- the administrator passwords for academy systems are kept in a secure place, e.g., academy safe.

- there is a risk-based approach to the allocation of learner usernames and passwords.
- there will be regular reviews and audits of the safety and security of academy technical systems.
- servers, wireless systems and cabling are securely located and physical access restricted.
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the academy systems and data. These are tested regularly. The academy infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.
- L.E.A.D. I.T Services are responsible for ensuring that all software purchased by and used by the academy is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, (as agreed).
- use of academy devices out of the academy and by family members is regulated by an acceptable use agreement that a user consents to when the device is allocated to them.
- personal use of any device on the academy network is regulated by acceptable use agreements that a user consents to when using the network.
- staff members are not permitted to install software on academy-owned devices.
- removable media is not permitted unless approved by the SLT/L.E.A.D. IT Services.
- systems are in place to control and protect personal data and data is encrypted at rest and in transit. (See personal data statement in the appendices for further detail).
- mobile device security and management procedures are in place. Under no circumstances should personal devices be used to access academy systems.
- guest users are provided with appropriate access to academy systems based on an identified risk profile and if required.

## Mobile technologies

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

*"The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e., 3G, 4G and 5G).*

*This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.*

Mobile technology devices may be academy owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of

utilising the academy's wireless network. The device then has access to the wider internet which may include the academy learning platform and other cloud-based services such as e-mail and data storage.

All users should be made aware that the primary purpose of the use of mobile/personal devices in an academy context is educational. This policy will be consistent with and inter-related to other relevant academy polices including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the academy's online safety education programme.

A range of mobile technology strategies is possible. However, these need to be thoroughly researched, risk assessed and aligned with existing policy prior to implementation. A more detailed mobile technologies statement can be found in the Appendices.

Birley Academy acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

We allow:

| | **School devices** | | | **Personal devices** | | |
|---|---|---|---|---|---|---|
| | School owned for individual use | School owned for multiple users | Authorised device[1] | Student owned | Staff owned | Visitor owned |
| Allowed in school | Yes | Yes | Yes | No | Yes | Yes |
| Full network access | Yes | Yes | Yes | No | No | No |
| Internet only | Yes | Yes | Yes | Yes | Yes | No |
| No network access | N/A | N/A | N/A | No | No | No |

**Academy owned/provided devices:**

- all Birley Academy devices are managed though the use of Mobile Device Management software.

[1] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed.
- any designated mobile-free zone is clearly signposted.
- personal use (for example, online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.
- the use of devices on trips/events away from the academy is clearly defined and expectation are well-communicated.
- liability for damage aligns with current academy policy for the replacement of equipment.
- education is in place to support responsible use.

**Personal devices:**

- there is a clear procedure covering the use of personal mobile devices on academy premises for all users.
- where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource.
- use of personal devices for academy business is defined in the acceptable use agreements and staff handbook. Personal devices commissioned onto the academy network are segregated effectively from academy-owned systems.
- the expectations for taking/storing/using images/video aligns with the academy's acceptable use agreements and use of images/video statement. The non-consensual taking/using of images of others is not permitted.
- liability for loss/damage or malfunction of personal devices is clearly defined.
- there is clear advice and guidance at the point of entry for visitors to acknowledge academy requirements.
- education about the safe and responsible use of mobile devices is included in the academy online safety education programmes.

**Social media**

With widespread use of social media for professional and personal purposes, we have a policy that sets out clear guidance for staff to manage risk and behaviour online.

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people at Birley Academy must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

We all have a duty of care to provide a safe learning environment for learners and staff. We could be held responsible, indirectly for acts of our employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the academy liable to the injured party. Reasonable steps to prevent predictable harm are in place.

Birley Academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.

- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.
- guidance for learners, parents/carers

Academy staff will ensure that:

- no reference should be made in social media to learners, parents/carers or academy staff.
- they do not engage in online discussion on personal matters relating to members of the academy community.
- personal opinions should not be attributed to the academy.
- security settings on their personal social media profiles are regularly checked to minimise risk of loss of personal information.
- they act as positive role models in their use of social media.

When official academy social media accounts are established, there is:

- a process for approval
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff.
- a code of behaviour for users of the accounts.
- systems for reporting and dealing with abuse and misuse…
- understanding of how incidents may be dealt with under academy disciplinary procedures.

### Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the academy it must be made clear that the member of staff is not communicating on behalf of the academy with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- personal communications which do not refer to or impact upon the academy are outside the scope of this policy.
- where excessive personal use of social media in the academy is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

### Monitoring of public social media

- As part of active social media engagement, we may pro-actively monitor the Internet for public postings about Birley Academy.
- when parents/carers express concerns about our academy on social media we will urge them to make direct contact with the academy, in private, to resolve the matter. Where this cannot be resolved, parents/carers will be directed to the academy complaints procedure.

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

The social media statement in Appendix C4 provides more detailed guidance on our responsibilities and on good practice.

### Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place.

Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. At Birley Academy, we will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- we may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies. Guidance can be found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education.
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners whose images must not be taken/published. **All** images should only be taken on academy devices. The personal devices of staff must not be used for such purposes
- In accordance with guidance from the Information Commissioner's Office, the academy will take video and digital images of children at academy events (with parental permission). Parents, may upon request, may have access to their child's individual images for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow our procedures concerning the sharing, storage, distribution and publication of those images.
- care should be taken when sharing digital/video images that learners are appropriately dressed.
- learners must not take, use, share, publish or distribute images of others without their permission.
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy.
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of learners are taken for use in our academy or published on the academy website/social media. (see parents and carers acceptable use agreement in the Appendix). Permission is not required for images taken solely for internal purposes.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the academy data protection policy.
- images will be securely stored in line with the academy retention policy.
- learners' work can only be published with the permission of the learner and parents/carers.

## Online Publishing

Birley Academy communicates with parents/carers and the wider community, and promotes the academy through:

- Public-facing website
- Social media
- Online newsletters

Our website is managed/hosted by LEAD IT. We ensure that the Online Safety Policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of academy calendars and personal information – ensuring that there is least risk to members of the academy community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

At Birley Academy, we ensure our online publishing provides information about online safety e.g., publishing the academy's Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the academy website.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process. (Report CEOP button)

## Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

Birley Academy:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so.
- has paid the appropriate fee to the Information Commissioner's Office (ICO).
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest. Our academy also has a Manager and Systems Controllers to support the DPO.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it.
- the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed.
- has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it.
- information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed.

- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The academy's 'retention schedule" supports this.
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- provides staff, parents, volunteers, teenagers, and older children with information about how the academy looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix).
- has procedures in place to deal with the individual rights of the data subject, e.g., one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them.
- carries out Data Protection Impact Assessments (DPIA) where necessary e.g., to ensure protection of personal data when accessed using any remote access solutions or entering into a relationship with a new supplier.
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors.
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data.
- reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- has a Freedom of Information procedure held within the GDPR policy.
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected.
- device will be password protected.
- device will be protected by up-to-date endpoint (anti-virus) software.
- data will be securely deleted from the device, in line with academy policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- can recognise a possible breach, understand the need for urgency and know who to report it to within the academy.
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to.

- only use encrypted data storage for personal data.
- will not transfer any academy personal data to personal devices. Academies have access to VPN and web remote access services to allow remote working safely and securely.
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

The Personal Data Advice and Guidance in the appendix (B2) provides more detailed information on our academy's responsibilities and on good practice.

### Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training.
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to academy leadership and governors.
- parents/carers are informed of patterns of online safety incidents as part of the academy's online safety awareness raising.
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate.
- the evidence of impact is shared with other academies, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

## Appendices

The appendices referred to in the policy are as follows:

A1 Learner Acceptable Use Agreement – for older learners
A2 Learner Acceptable Use Agreement – KS2
A3 Learner Acceptable Use Agreement – for younger learners (Foundation/KS1)
A4 Parent/Carer Acceptable Use Agreement
A5 Staff (and Volunteer) Acceptable Use Agreement
A6 Community Users Acceptable Use Agreement
A7 Online Safety Group Terms of Reference Template
A8 Harmful Sexual Behaviour statement
A9 Responding to incidents of misuse – flow chart
A10 Record of reviewing devices/internet sites (responding to incidents of misuse)
A11 Reporting Log
B1 Training Needs Audit Log

C1 Technical Security statement (including filtering and passwords)
C2 Personal Data Advice and Guidance
C3 Academy Online Safety statement; Electronic Devices - Searching Screening and Confiscation (new DfE guidance from September 2023)
C4 Mobile Technologies statement (inc. BYOD/BYOT)
C5 Social Media statement

Legislation
Links to other organisations and resources
Glossary of Terms

*The appendices are not included in the online version of the website, but are available by request to the headteacher.*