Self-help
Self-responsibility
Equity
Equality
Democracy
Solidarity

Osborne
Co-operative Academy Trust

Policy/Procedure: Online and Information and Communication Technology Policy

Review Frequency: Every Two Years

Date of last review: 2nd April 2019

Date of next review: April 21

1. Introduction and Overview 4
2. Education and Curriculum 9
3. Expected Conduct and Incident Management 10
4. Managing IT and Communication Systems 11
5. Data Security - Management Information System access and data transfer 16
6. Equipment and Digital Content 17
7. Appendices 19

Osborne Co-operative Academy Trust is a multi-academy trust (MAT) incorporated around the principles and values of the international co-operative movement. These are Equality, Equity, Democracy, Self-help, Self-Responsibility and Solidarity, along with the ethical values of openness, honesty, social responsibility and caring for others. These values and principles underpin all our actions.

Introduction

This policy will be personalised and adopted for use by the Osborne Co-operative Academy Trust's individual schools and is linked to the Acceptable Use Policies.

The online safety policy is linked to other policies in schools, including: Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy and Social Media policy.

Monitoring, Evaluation and Review

This policy will be promoted and implemented throughout the Trust. The board will review the policy annually, unless there are significant legislative changes in the interim period.

The Trust and each individual school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students / pupils
    - parents / carers
    - staff

Policy reviewed: February 2019

Signed _____

On behalf of Osborne Co-operative Academy Trust

Date _____

This policy was adopted by the Local Governing Body of _____

Signed _____

On behalf of the Local Governing Body

Date _____

1. Introduction and Overview

The purpose of this policy is to:

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

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

Content

- Exposure to inappropriate content
- Websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

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

Conduct

- Aggressive behaviours
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

1.1. Scope

This policy applies to all members of Osborne Co-operative Academy Trust community (including staff, Trustees, Local Governors, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school IT systems, both in and out of the Osborne Co-operative Academy Trust.

1.2. Roles and Responsibilities

Role	Key Responsibilities
Chief Executive Officer	- Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance;

	- To lead a 'safeguarding' culture across the Trust, ensuring that online safety is fully integrated and of high priority; - To take overall responsibility for data management and information security (Trust SIRO) ensuring academy's relevant Local Safeguarding Children Board (LSCB) guidance - To ensure that key ICT strategies are discussed through the ICT Special Interest Group and delivered back to the Trust Board and or Headteacher/Head of Schools and Schools. - To ensure that all school leaders are aware of procedures to be followed in the event of a serious online safety incident; - To ensure the Trust Board are regularly updated on the nature and effectiveness of the school's arrangements for online safety; - To hold schools to account for the effectiveness of their on-line safety.

Headteacher or Head of school	- Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance;
	- To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding;
	- To take overall responsibility for online safety provision;
	- To take overall responsibility for data management and information security as the Senior Information Risk Owner (SIRO) ensuring academy's relevant Local Safeguarding Children Board (LSCB) guidance.
	  ○ Establish an effective Information Governance Framework
	  ○ Act as the champion for information risk within your organisation, being an exemplar for all staff and encouraging the Leadership Team to do likewise
	  ○ Build networks with peers and organisations that can provide essential support and knowledge exchange services
	  ○ Ensure compliance with regulatory, statutory and organisational information security policies and standards
	  ○ Ensure all staff are aware of the necessity for information assurance and of the risks affecting the organisation's corporate information
	  ○ Establish a reporting and learning culture to allow the organisation to understand where problems exist and develop strategies (policies, procedures and awareness campaigns) to prevent problems occurring in the future.
	- To ensure the school uses appropriate IT systems and services including, filtered Internet Service. This will be done under the guidance of the school or trust network manager with support from the trust SIG;
	- To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles;
	- To be aware of procedures to be followed in the event of a serious online safety incident;
	- Ensure suitable 'risk assessments' are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised;
	- To ensure all staff responsible for online safety systems are adequately monitored and supported by the school network manager, or the Trust network manager in the case of school network managers;
	- To ensure Local Governing Bodies are regularly updated on the nature and effectiveness of the school's arrangements for online safety;

	- To ensure school website includes relevant and statutory information.
Online Safety Coordinator/ Designated Child Protection Lead (This may be the same person)	- Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's safety policy/documents - Promote an awareness and commitment to online safety throughout the school community; - Ensure that online safety education is embedded within the curriculum; - Liaise with Osborne Co-operative Academy Trust technical staff where appropriate; - To communicate regularly with the schools Senior Leadership Team and the designated online safety governor/committee to discuss current issues, review incident logs and filtering and change control logs; - To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident; - To ensure that online safety incidents are logged as a safeguarding incident; - Facilitate training and advice for all staff; - Oversee any pupil surveys / feedback on online safety issues; - Liaise with the Local Authority and relevant agencies; - Is regularly updated in online safety issues and legislation and be aware of the potential for serious child protection concerns.
School Local Governing Body member responsible for Online Safety (or responsible for Safeguarding to include Online Safety)	- To ensure that the school has in place policies and practices to keep the children and staff safe online; - To approve the Trust's Online Safety Policy and the School's individual policy and review the effectiveness of them; - To support the school in encouraging parents and the wider community to become engaged in online safety activities; - To conduct regular online safety reviews with the school online safety coordinator.
Computing Curriculum Leader	- To oversee the delivery of the online safety element of the Computing curriculum in each school.

Trust/School Network Manager /technician	- To report online safety related issues that come to their attention, to the Online Safety Coordinator/Designated Safeguarding Lead in school using the incident report form and update the summary log;
	- To manage the schools/whole Trust network and make sure that:
	  o School/trust password policy is strictly adhered to and reset a minimum of twice a year for all users
	  o Systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date);
	  o Access controls/encryption exist to protect personal and sensitive information held on school-owned devices;
	  o The school's policy on web filtering is applied and updated on a regular basis.
	- Keep up to date with the School's and Trust online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant;
	- School technology and online platforms are regularly monitored, and any misuse/attempted misuse is reported to the online safety coordinator/Headteacher/Head of School;
	- To ensure appropriate backup procedures and disaster recovery plans are in place;
	- To keep up-to-date documentation of the disaster recovery plans.
	- To keep key staff updated and abreast of current threats and trends with online security. Educating staff and updating on potential risks.

Data and Information (Asset Owners) Managers (IAOs)	- To ensure that the data they manage is accurate and up-to-date; - Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements; - The Trust must be registered with Information Commissioner. - The Trust and individual schools demonstrate ongoing compliance to GDPR and annual reviews carried out on behalf of the data protection officer show this.
Teachers	- To embed online safety in the curriculum; - To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant); - To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws. - To ensure that pupils have an understanding of the school's acceptable use policy, as appropriate to their age, and are supported to follow the policy when using technology - To ensure that all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems - they 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.
All staff, volunteers and contractors.	- To annually read, understand, sign and adhere to: - OCAT GDPR Data Protection Policy - OCAT GDPR Acceptable personal use Policy - OCAT GDPR Data handling security Policy - OCAT GDPR Records management Policy - Polices are signed for by new staff on induction using the EVERY system; - To report any suspected misuse or problem to the online safety coordinator;

	- To maintain an awareness of current online safety issues and guidance e.g. through CPD; - To model safe, responsible and professional behaviours in their own use of technology. - At the end of the period of employment/volunteering to return any equipment or devices loaned by the Academy or Trust. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Pupils	- Read, understand, sign and adhere to the relevant Student/Pupil Acceptable Use Policy agreement at the beginning of each key stage and follow any updates - To understand the importance of reporting abuse, misuse or access to inappropriate materials; - To 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 behaviours and good online safety practice when using digital technologies out of the school - To have the opportunity to become Digital Leaders (or similar); - To have a good age appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations; - Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
Parents/ carers	- To read, understand and promote the school's Student/Pupil Acceptable Use Policy agreement with their child/children; - To read, understand and adhere to the parents/carers Acceptable Use Policy agreement; - To consult with the school if they have any concerns about their children's use of technology;
External groups including Parent groups	- Any external individual/organisation will sign an Acceptable Use Policy agreement prior to using technology or the Internet within the school; - To support the school and Trust in promoting online safety; - To model safe, responsible and positive behaviours in their own use of technology.

1.3. Communication:

The policy will be communicated to staff, pupils and the community in the following ways:

- Policy to be posted on individual schools' website, staffroom, classrooms and on the Trust website.
- Policy to be part of induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

1.4. Handling Incidents:

- The school and Trust will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Online Safety Co-coordinator or the Designated Safeguarding Lead act as first point of contact for any incident. They can be supported if necessary by the school GDPR Information Champion

- Any suspected online risk or infringement is reported to Online Safety Coordinator/Headteacher/Head of School that day.
- Any concern about staff misuse is always referred directly to the Headteacher/Head of School, unless the concern is about the Headteacher/Head of School in which case the compliant is referred to the Chair of the Local Governing Body.
  (See Appendix 3 - Online Safety Infringements and Sanctions)

2. Education and Curriculum

2.1. Pupil online safety curriculum

Osborne Co-operative Academy Trust and individual schools:

- Has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- Plans online use carefully to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas;
- Will remind pupils about their responsibilities through the student/pupil Acceptable Use Policy Agreement(s);
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright, use of social media;
- Ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- Ensure pupils only use school approved systems and publish within appropriately secure / age-appropriate environments.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. Nb. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities. Each school should take part in and promote the annual National Internet Safety week activities.

2.2. Staff and governor training

Osborne Co-operative Academy Trust and its individual schools:

- Make regular training available to staff on online safety issues and the school's online safety education program;
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Policy Agreements.
- An audit of the online safety training needs of all staff will be carried out regularly.
- Governors / Directors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:
  - Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).
  - Participation in school / Trust training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

2.3. Parent awareness

Osborne Co-operative Academy Trust and its individual schools:

- Take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:
    - digital and video images taken at school events
    - access to parents' sections of the website / Learning Platform and on-line student / pupil records
    - their children's personal devices in the school (where this is allowed)

2.4. The Wider Community

The schools and the Trust will provide opportunities for local community groups / members of the community to gain from the Trust's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision

3. Expected Conduct and Incident Management

3.1. Expected conduct

In Osborne Co-operative Academy Trust all users:

- Are responsible for using the school IT and communication systems in accordance with the OCAT GDPR Acceptable personal use policy
- Understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- Understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so;
- Understand the importance of adopting good online safety practice when using digital technologies in and out of the school;
- Know and understand academy policies on the use of mobile and hand-held devices including cameras.

3.2. Staff, volunteers and contractors

- Know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;
- Where available use appropriate technology to help monitor pupils internet usage such as RM tutor.

3.3. Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety Acceptable Use Policy Agreement;
- Should know and understand what the school's rules of appropriate use for the whole school community are and what sanctions result from misuse.

3.4. Incident Management

In the Osborne Co-operative Academy Trust and individual schools:

- There is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- All members of the academy Trust are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- Support is actively sought from other agencies as needed (e.g. UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, Internet Watch Foundation) in dealing with online safety issues;
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the schools (appendix 3);
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation, CEOP etc.

Monitoring

Logs of filtering change controls and of filtering incidents will maintained by the Network Manager. These should be kept in a secure location and made available should they be requested by any board, governing body or senior staff member for monitoring purposes.

There are a range of monitoring strategies and systems which are in place at the Osborne Co-operative Academy Trust and its schools including:

- Physical Monitoring
- Internet and web access
- Monitoring content
- Monitoring strategy/System features

4. Managing IT and Communication Systems

4.1. Internet access, security (virus protection) and filtering

Osborne Co-operative Academy Trust and its individual schools:

- Inform all users that Internet/email use is monitored;
- Has filtered secure broadband connectivity as advised by the Trust network manager;
  - The Trust broadband access will include filtering appropriate to the age and maturity of pupils either directly through broadband provider or 3rd party solutions;
  - The Trust Network Manager will work with the Broadband provider to ensure that filtering procedures are continually reviewed;
  - The academy trust will have a clear procedure for reporting breaches of filtering. All members of the academy community (all staff and all pupils) will be aware of this procedure through acceptable use policies and training (appendix 3);
  - If staff or pupils discover unsuitable sites, the URL will be reported to the Trust Network Manager who will then record the incident and escalate the concern as appropriate;
  - The filtering system will block all sites on the Internet Watch Foundation (IWF) list;

- Changes to the school filtering procedures will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team;
- The Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective;
- Any material that the school believes is illegal will be reported to appropriate agencies such as Internet Watch Foundation, the Police or CEOP;
- The access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers;
- Changes to the filtering policies are updated by the Network Manager as directed by the Senior Leadership Team;

- Ensure network health through use of suitable anti-virus software;
- Use DfE/Local Authority approved systems to send 'protect-level' sensitive / personal data over the Internet;
- Use encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet**.**

4.2. Network management (user access, backup)

Osborne Co-operative Academy Trust and its individual schools:

- Use individual, audited logins for all users;
- Use guest accounts occasionally for external or short-term visitors for temporary access to appropriate services;
- Use teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful;
- Has daily back-up of school data (admin and curriculum);
- Use secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Storage of all data within the school will conform to the EU and UK data protection requirements (GDPR); Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, Osborne Co-operative Academy Trust and its individual schools:

- Ensures staff read and sign that they have understood this online safety policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password;
- All pupils have their own unique username and password which gives them access to the Internet and other services;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with shared drives and O365 work areas. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities;
- Maintains equipment to ensure Health and Safety is followed;
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;

- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- The Trust and Schools use secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
  All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards.

4.3. Password policy

Osborne Co-operative Academy Trust make it clear that staff and pupils must always keep their passwords private, must not share with others;

- If a password is compromised the Trust Network Manager should be notified immediately;
- All staff have their own unique username and private passwords to access systems. Staff are responsible for keeping their password(s) private;
- We require staff to use STRONG passwords;
- We require staff to change their passwords a minimum of twice per year;
- We require staff using critical systems to use two factor authentication.
- The management of password security will be the responsibility of the Trust Network Manager.

4.3.1. Responsibilities:

All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Passwords for new users, and replacement passwords for existing users can be allocated by the School or Trust Network Manager. Any changes carried out must be notified to the member of staff responsible for issuing and coordinating password security (above).

4.3.2. Training/Awareness:

It is essential that users are made aware of the need to keep passwords secure, and the risks attached to unauthorised access/data loss. This should apply to even the youngest of users, even if class logons are being used.

Members of staff will be made aware of the Trust's password security procedures:

- at induction;
- through the academy's Online Safety Policy and procedures;
- through the OCAT GDPR Acceptable Personal Use policy;

Pupils will be made aware of the Trust's password security procedures:

- in ICT and/or Online Safety lessons
- through the Acceptable Use Policy Agreement

The following rules apply to the use of passwords:

- the last four passwords cannot be re-used;
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special character;
- the account should be "locked out" following six successive incorrect log-on attempts;
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on;
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption);

- requests for password changes should be authenticated to ensure that the new password can only be passed to the genuine user;

The "master/administrator" passwords for the school ICT system, used by the Trust Network Manager must also be available to the CEO or other nominated senior leader and kept in a secure place (e.g. Trust safe). Alternatively, where the system allows more than one "master/administrator" log-on, the CEO or other nominated senior leader should be allocated those master/administrator rights. The Trust should never allow one user to have sole administrator access.

4.3.3. Audit/Monitoring/Reporting/Review:

The Trust or local schools Network Manager will ensure that full records are kept of:

- User IDs and requests for password changes;
- User logons;
- Security incidents related to this Policy and procedures.

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption. Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner. These records will be reviewed by the (Online Safety Coordinator/Online Safety Governor) at regular intervals.
If any incidents of misuse occur, these should be reported using the flow chart and forms in appendix 3.

4.4. E-mail

Osborne Co-operative Academy Trust and its individual schools:

- Provides staff and, where appropriate, pupils with an email account for their professional use. Personal email should be through a separate account and not accessed through School devices;
- Uses anonymous or group e-mail addresses, for example info@stcleres.coop;
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law;
- Will ensure that email accounts are maintained and up to date;
- Use a number of technologies to help protect users and systems in the school;
- Ensure staff will only use official school provided email accounts to communicate with pupils and parents, as approved by the Senior Leadership Team;
- Ensure the forwarding of chain messages is not permitted;
- Ensure the official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the Trust email service to communicate with others when in school, or using secure remote access.
- Email on phones and other devices should only be accessed via a secure, approved and password protected app.
- Users need to be aware that email communications may be monitored.

4.4.1. Emailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using email - emailing confidential data is not recommended and should be avoided where possible. Use should be made in O365 of shared files or folders which can only be accessed by the recipient not via a link which could be forwarded to anyone;
- The use of Hotmail, BT Internet, G-mail or any other Internet based webmail service for sending email containing sensitive information is not permitted;
- Where your conclusion is that email must be used to transmit such data:
    - Obtain express consent from your manager to provide the information by email;

- Exercise caution when sending the email and always follow these checks before releasing the email:
    - Verify the details, including accurate email address, of any intended recipient of the information;
    - Verify (by phoning) the details of a requestor before responding to email requests for information;
    - Do not copy or forward the email to any more recipients than is absolutely necessary.
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone);
- Send the information as an encrypted document attached to an email;
- Provide the encryption key or password by a separate contact with the recipient(s);
- Do not identify such information in the subject line of any email;
- Request confirmation of safe receipt.

Pupils:

- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff can only use the trust e mail account provided and no others when communicating in relation to their role;
- Staff will use the e-mail systems only for professional purposes;
- Access in Trust to external personal email accounts may be blocked;
- Never use email attachments to transfer staff or pupil personal data or any 'Protect-level' data. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption or use should be made in O365 of shared files or folders which can only be accessed by the recipient not via a link which could be forwarded to anyone;

4.5. Websites

- The CEO and/or the Headteacher/Head of Schools, supported by the Trust Board and Local Governing Bodies, takes overall responsibility to ensure that the website content is accurate, and the quality of presentation is maintained;
- All websites comply with statutory DFE requirements;
- Most material is the Trust/School's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website, permission is sought from parents/carers;

4.6. Cloud Environments

- Uploading of information on the school's online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;
- In the school, pupils are only able to upload and publish within school's approved 'Cloud' systems.

4.7. Social networking

Please refer to "**Social Media Policy**: Staff

4.7.1. Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate;
- Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open up their own spaces to their pupils, but to use the Trust/School's preferred system for such communications. (please refer to the Trust Communication Policy)

4.7.2. Pupils

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work;
- Pupils are required to sign and follow our [age appropriate] Pupil Acceptable Use Policy Agreement.

4.7.3. Parents

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Policy Agreement and additional communications materials when required;
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.
- Parents are advised at school events not to share photos/videos from the event on social media.

4.8. Recording Equipment

- Schools utilise a range of recording equipment for a variety of purposes, such as security surveillance, public task records and school improvement.
- Recording equipment will only be used for the purpose(s) for which it was intended and all recordings will only be stored and shared according to current GDPR regulations (refer also to Trust policies relating to GDPR)

4.9. Disposal of Redundant ICT Equipment

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.
    - Disposal of any ICT equipment will conform to:
        - The Waste Electrical and Electronic Equipment Regulations 2006
        - The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
        - Environment Agency Guidance (WEEE) Click here to access
        - ICO Guidance - Data Protection Act 1998 Click here to access
        - Electricity at Work Regulations 1989
    - Each school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.
    - The school's disposal record will include:
        - Date item disposed of;
        - Authorisation for disposal, including:
            - verification of software licensing
            - any personal data likely to be held on the storage media? *
        - How it was disposed of e.g. waste, gift, sale
        - Name of person and/or organisation who received the disposed item

* if personal data is likely to be held the storage media will be over written multiple times or 'scrubbed' to ensure the data is irretrievably destroyed.

- Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

5. Data Security - Management Information System access and data transfer

5.1. Strategic and operational practices

At Osborne Co-operative Academy Trust:

- We aim to be compliant with GDPR
- There is a nominated Data Protection Officer (DPO).
- We ensure staff know who to report any incidents where data protection may have been compromised;
- All staff are DBS checked and records are held in a single central record.

5.2. Technical Solutions

- Staff have secure area(s) on the network to store sensitive files;
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes' idle time;
- All servers are in secure locations, either a locked cabinet or locked room, and managed by DBS-checked staff;
- Details of all school-owned hardware will be recorded in a hardware inventory;
- Details of all school-owned software will be recorded in a software inventory;
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website;
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data;
- We use secure file deletion software.

6. Equipment and Digital Content

6.1. Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into schools are entirely at the staff member, pupil's & parent's or visitor's own risk. The Trust/School accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school;
- Mobile devices are not permitted to be used in certain areas within the school's sites, e.g. changing rooms and toilets.
- Mobile devices brought in to the school are the responsibility of the device owner. The Trust/School accepts no responsibility for the loss, theft or damage of personally-owned mobile devices;
- Older pupils in our Secondary Schools may be invited to bring mobile phone or personally-owned devices into the school as part of the 'Bring Your Own Device' initiative.
    - If this is the case, personal mobile devices will only be used during lessons with permission from the teacher;
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned;
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher/Head of School. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher/Head of School is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary;

- The Trust reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.

Pupils' use of personal devices

- If a pupil needs to contact his or her parents or carers, they will be allowed to use the school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office;
- If a pupil breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations;
- Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting;
- Staff will be issued with a Trust/School phone where contact with pupils, parents or carers is required, for instance for off-site activities;
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances or for approved educational purposes;
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose. The exception to this is when teachers are using an approved app for educational purposes, which must be:
    - 1. Approved by the Headteacher/Head of School
    - 2. Where the image(s) are stored only in professional O365 cloud areas and are deleted off the local device as soon as practicable
    - 3. Where images don't make the pupils identifiable e.g. have names attached without express permission from the parent/carer, or pupil for those over 16
    - 4. Where staff ensure no visible images of pupils who are on a "No Photos Allowed" list are used;
- In an emergency where a staff member needs to make a call and doesn't have access to an Trust/School-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes and then report the incident with the Headteacher/Head of School;
- If a member of staff breaches the Trust/School policy then disciplinary action may be taken.
- Staff may use their phones during non-contact times and in a location not visible or audible to pupils. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf or seek specific permissions from the Headteacher/Head of School to use their phone at other than non-contact times.

6.2. Storage, Synching and Access

If the device is accessed with as Trust/School owned account

- The device has a Trust/School created account and all apps and file use is in line with this policy. No personal elements may be added to this device;
- PIN access to the device must always be known by the network manager;

If the device is accessed with a personal account

- If personal accounts are used for access to Trust/School owned mobile device, staff must be aware that work use will be synched to their personal cloud, and personal use may become visible in Trust/School and in the classroom;
- PIN access to the device must always be known by the network manager;
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse;

6.3. Digital images and video

In Osborne Co-operative Academy Trust:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school;
- We do not identify pupils in generic online photographic publicity materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Photographs of pupils with names may be used for publicity purposes only with signed agreement from the pupil or parent (if under 16), such as publishing a name and image of a pupil reaching a sporting event national final;
- Staff sign the Trust's Acceptable Use Policy Agreements, and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the Trust/School website, in the prospectus or in other high-profile publications the school will obtain individual parental or pupil permission for its long term, high profile use;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make their personal information public;
- Pupils are taught that they should not post images or videos of others without their permission. They should be taught about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

7. Appendices

Appendix 1 - Online Safety Resources
Appendix 2 - Online Infringements and Sanctions
Appendix 3 – Responding to incidents misuse flow chart

Appendix 1 -

Online Safety Resources

National Agencies

- Child Exploitation and Online Protection centre CEOP's homepage - report concerns to CEOP via the "Click Ceop" button
- Virtual Global Taskforce - VGT homepage
- Think U Know - Advice for Parents, Teachers and Young people and teaching resources
- Internet Watch Foundation - Report illegal Content online
- Childnet International – Guidance for Parents, Teachers, Children and Young People
- UK Safer Internet Centre
- NEN E-Safety
- NSPCC

e-Safety Curriculum Materials

- ThinkUKnow - Material from CEOP aimed at children aged 4 to 16 (KS1/2/3/4)
- All about Explorers - Evaluate reliability of online information (KS2/3)
- Create a Buddie - Primary tool and Secondary tool (Use the Demo version to avoid registering)
- Websafecrackerz - Online activities (KS2/3)
- Welcome to the Web (KS2/3)
- Ideas to Inspire Internet Safety
- Webwise - resource from Ireland (KS2/3)
- e-Safety Games Online Games from the North West Learning Grid (KS2/3)
- Young People Safe online - Advice and Resources for Young People (KS2/3)
- The Quality Information Checklist - Useful tool to check websites (KS2/3)
- Kidsmart - Activities, Videos and information (KS1/2/3)
- ChildLine Online Safety Advice
- Information Comissoners Office - Guidance for Young People (KS3/4)
- I Keep Safe - (KS1/2/3/4)
- Netsmartz - (KS1/2/3/4)
- Get Netwise - (KS2/3/4)

For Parents

- Think U Know: Parents/carers Guide to the Internet
- Direct Gov: Internet Safety - Advice for parents
- Get Safe Online - Advice and guidance on Safety online
- Go On - Free online learning course about basic Internet skills and safety
- Digital Parenting Magazine - Advice from Industry for Parents/carers
- Disney's Online Safety
- Yahoo Safety Tips
- Google Family Safety
- Microsoft UK Safety and Security Centre
- Click CEOP Browser Safety Tools - Download the Click CEOP button onto web browsers
- Common Sense Media - American site which reviews websites, games
- BBC Webwise - Online Basics from the BBC
- BBC Webwise "Share Take Care" - Guidance for parents/carers on Social Networking
- NetLingo – Common Online acronyms and text speak e.g. LOL, POS
- Parents' Guide to Facebook

Appendix 2 - Online Safety Infringements and Sanctions

Online Safety Infringements and Sanctions

(These may be adapted in individual schools within the Trust)

PUPIL	
Category A infringements	**Possible Sanctions:**
• Use of non-educational sites during lessons • Unauthorised use of email • Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends • Use of unauthorised instant messaging / social networking sites	**Refer to class teacher / tutor** Escalate to: senior manager / Online-Safety Coordinator
Category B infringements	**Possible Sanctions:**
• Continued use of non-educational sites during lessons after being warned • Continued unauthorised use of email after being warned • Continued unauthorised use of mobile phone (or other new technologies) after being warned • Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups • Use of File sharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc. • Trying to buy items over online • Accidentally corrupting or destroying others' data without notifying a member of staff of it • Accidentally accessing offensive material and not logging off or notifying a member of staff of it	**Refer to Class teacher/ Head of Department / Year tutor / Online-Safety Coordinator** Escalate to: removal of Internet access rights for a period / removal of phone until end of day / contact with parent]
Category C infringements	**Possible Sanctions:**
• Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site. • Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off) • Trying to access offensive or pornographic material (one-off) • Purchasing or ordering of items online • Transmission of commercial or advertising material • Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned	**Refer to Class teacher / Year Tutor / Online-Safety Coordinator / Headteacher/Head of School / removal of Internet and/or Learning Platform access rights for a period** Escalate to: contact with parents / removal of equipment **Other safeguarding actions**

• Deliberately creating accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988 • Bringing the school name into disrepute	**if inappropriate web material is accessed:** Ensure appropriate technical support filters the site **Refer to Headteacher / Contact with parents** **Other possible safeguarding actions:** • Secure and preserve any evidence • Inform the sender's e-mail service provider. • Liaise with relevant service providers/ instigators of the offending material to remove • Report to Police / CEOP where child abuse or illegal activity is suspected

(How will infringements be handled? If the Online-Safety Policy has been infringed, the final decision on the sanction is with the Trust/Schools's senior management.

STAFF	
Category A infringements (Misconduct)	**Possible Sanctions:**
• Excessive use of school Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc. • Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored. • Not implementing appropriate safeguarding procedures. • Any behaviour on the World Wide Web that compromises the staff members' professional standing in the school and community. • Misuse of first level data security, e.g. wrongful use of passwords. • Breaching copyright or license e.g. installing unlicensed software on network.	**Referred to line manager / Headteacher/Head of School** Escalate to: *Warning given*
Category B infringements (Gross Misconduct)	**Possible Sanctions:**

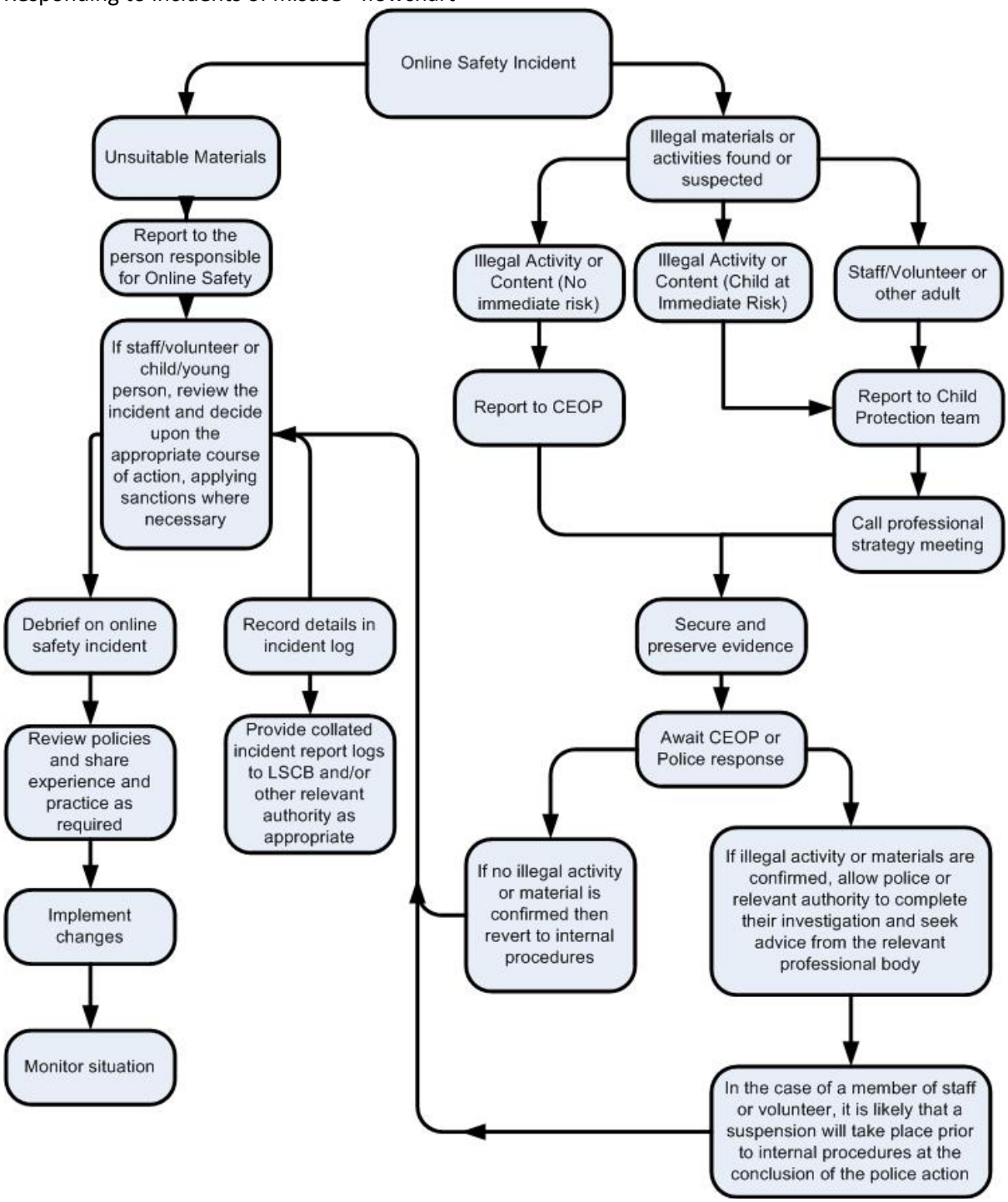
• Serious misuse of, or deliberate damage to, any school / Trust computer hardware or software; • Any deliberate attempt to breach data protection or computer security rules; • Deliberately creating, accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent; • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988; • Bringing the school name into disrepute	**Referred to Headteacher / Governors**; Other safeguarding actions: • Remove the PC to a secure place to ensure that there is no further access to the PC or laptop. • Instigate an audit of all ICT equipment by an outside agency, such as the school's ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school. • Identify the precise details of the material. • Escalate to: • Report to LA /LSCB, Personnel, Human Resources. • Report to Police / CEOP where child abuse or illegal activity is suspected.

If a member of staff commits an exceptionally serious act of gross misconduct The member of staff should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken. The School are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Trust Human Resources team. The Headteacher/Head of School should also report such incidents to the LADO if appropriate, as well as ensuring the incident log is completed.
Child abuse images found In the case of Child abuse images being found, the member of staff should be **immediately suspended** and the Police should be called. Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP): http://www.ceop.gov.uk/reporting_abuse.html

How will staff and pupils be informed of these procedures?

- They will be fully explained and included within the school's online-safety acceptable use agreement form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop unacceptable behaviours'.
- Pupils will sign an age appropriate online-safety / acceptable use policy agreement form;
- The Trust and School's online-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc. will be made available by the school for pupils

Appendix 3 -
Responding to incidents of misuse - flowchart



Osborne Co-operative Academy Trust

ONLINE INCIDENT REPORT FORM

Completed by: **Role:**	**Date of incident:**
Location:	**Time of incident:**
Time and date incident was logged:	

Details of people involved (children, staff, family members)

Please include names, genders, ages, ethnic origin, and children in care or children with special needs and each child's role - ringleader, outsider, reinforcer, assistant, defender, victim - and level of involvement.

1 = very involved 2 = involved 3 = slightly involved 4 = only indirectly involved

E-Safety incident related to: tick all that apply

Bullying or harassment (Cyber-bullying)		Racist, sexist, homophobic religious hate material	
Terrorist material		On-line gambling	
Deliberately bypassing security or access		Soft core pornographic material	
Drug/bomb material		Illegal hard core pornographic material	
Hacking or virus propagation		Other (please specify)	
Child abuse material			

Details of incident: Please write about exactly what you witnessed. If you were told information, please record that and who said it. Please attach any relevant supporting evidence.

Actions taken:

Involving Staff-

Incident reported to Headteacher/Head of School/senior manager	
Advice sought from Safeguarding and Social care	
Referral made to Safeguarding and Social care	
Incident reported to police	
Incident reported to other organisation (i.e CEOP)	
Incident reported to IT	
Disciplinary action to be taken	
E-Safety policy to be reviewed/amended	

Involving Child/Young person –

Incident reported to Headteacher/Head of School/senior manager	
Advice sought from Safeguarding and Social care	
Referral made to Safeguarding and Social care	
Incident reported to police	
Incident reported to other organisation (i.e CEOP)	
Incident reported to IT	
Child's parents informed	
Disciplinary action to be taken	
Child/young person debriefed	
E-Safety policy to be reviewed/amended	

Notes:

Completed by:…….

Role:……. Date:…….

Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		