CASTLEFIELD SCHOOL

E-SAFETY POLICY

Signed (HT): 

Date agreed: Term 3 2022

Signed (Chair of GB): 

Review date: Term 3 2025

Contents

Appendices:

1. Introduction and Overview

Rationale
This policy takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2022, 'Early Years and Foundation Stage' 2022 and 'Working Together to Safeguard Children' 2018.

Commented [JW1]: Dates changes

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Castlefield School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Castlefield School.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and codes of practice relevant to the responsible use of the internet for educational, personal or recreational use.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.
- Identify clear procedures to use when responding to online safety concerns and have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.

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

Content: being exposed to illegal, inappropriate or harmful material

- Exposure to inappropriate content, including online pornography, substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites and extremist material
- Content validation: how to check authenticity and accuracy of online content

Contact: being subjected to harmful online interaction with other users

- Grooming
- Cyber-bullying in all forms
- Identity theft and sharing passwords

Conduct: personal online behaviour that increases the likelihood of, or causes, harm

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (internet or gaming))
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

Scope
This policy applies to all members of Castlefield School community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of Castlefield School ICT systems, both in and out of school.

Castlefield School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.

Castlefield School believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.

The Education and Inspections Act 2006 empowers headteachers to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles • To be aware of procedures to be followed in the event of a serious e-safety incident • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager) • Educating Parents and raising awareness
Computing Lead and Designated Safeguarding Lead	• Take day to day responsibility for e-safety issues and has a leading role in reviewing the school e-safety policies / documents • Promotes an awareness and commitment to e-safeguarding throughout the school community • Ensures that e-safety education is embedded across the curriculum • Liaises with school ICT technical staff • To communicate regularly with SLT and the designated e-safety Governor to discuss current issues, review incident logs and filtering control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident • Facilitates training and advice for all staff • Liaises with the Local Authority and relevant agencies • Is regularly updated in e-safety issues and legislation, and is aware of the potential for serious child protection issues to arise from: • sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming • cyber-bullying and use of social media

Commented [JW2]: Changed from 'Child Protection Officer'

Role	Key Responsibilities
Governors / e-safety governor	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the e-safety Policy and review the effectiveness of the policy. This will be carried out by the Governors Curriculum Committee receiving regular information about e-safety incidents and monitoring reports. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities
Computing Curriculum Leader	• To oversee the delivery of the e-safety element of the computing curriculum • To liaise with the e-safety coordinator regularly
Network Manager/ technician	• To report any e-safety related issues that arises, to the e-safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • To ensure the school's policy on web filtering is applied and updated on a regular basis • Inform *Turn IT On* of issues relating to the filtering applied by them • Keep up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • Ensure that the use of the network, remote access and email is regularly monitored in order that any misuse / attempted misuse can be reported to the e-safety Co-ordinator / Headteacher for investigation, action and sanction where appropriate • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extracurricular 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 always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
All staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement • To be aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation. • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the e-safety coordinator • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, social media, text, mobile phones etc.

Commented [JW3]: Changed from 'Sub'

Commented [JW4]: This does not come from governors!

Commented [JW5]: This is not a role in school

Commented [JW6]: Not currently part of ay induction I carry out. Is it in new starter pack?

Role	Key Responsibilities
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Agreement (N.B. at KS1 it is expected that parents / carers sign on behalf of the pupils) • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • 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 know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • To respect the feelings and rights of others both on and offline. • To take responsibility for keeping themselves and others safe online. • To seek help from a trusted adult, if there is a concern online.
Parents/carers	• To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images • To read, understand and promote the school Pupil Acceptable Use Agreement with their children • To consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school

Commented [JW7]: Should this be revisited more often? Annually?

Communication:
How the policy will be communicated to staff, pupils and community:

- Policy to be posted on the school website and on the school network
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to pupils and staff on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

Handling complaints:

- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, nor any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - Interview/counselling by tutor / Head of Year / Computing Subject Leader / Headteacher;
  - Informing parents or carers;
  - Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system];
  - Referral to LA / Police.

- Our headteacher acts as first point of contact for any complaint, including any complaint about staff misuse.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures, this includes Prevent issues.

Review and Monitoring

- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.

- The e-safety policy has been written by the school e-safety coordinator and is current and appropriate for its intended audience and purpose.

Commented [JW8]: ???

2. Education and Curriculum

Pupil e-safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing curriculum. It is built on Kapow Computing scheme of work. This covers a range of skills and behaviours appropriate to age and experience, including:

Commented [JW9]: Changed from 'Rising Stars, SwitchedOn Computing'

  - to STOP and THINK before they CLICK, and to be SMART on the Internet,
  - to understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
  - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
  - to be aware that the author of a web site or page may have a particular bias or purpose and to develop skills to recognise what that may be;
  - to know how to narrow down or refine a search;
  - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
  - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos;
  - to understand why they must not post pictures or videos of others without their permission;
  - to know not to download any files – such as music files - without permission;
  - to have strategies for dealing with receipt of inappropriate materials;
  - To understand the impact of cyberbullying, and know how to seek help if they are affected by any form of online bullying.
  - To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or

carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

- Plans Internet 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 an end-user Acceptable Use Policy which every pupil will sign.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;

Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.
- Makes regular training and information available to staff on e-safety issues and the school's e-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 e-safety policy and the School's Acceptable Use Agreements.

Commented [JW10]: Those who need to know, know

Commented [JW11]: I know regular doesn't mean frequent, but I can't remember when we last had training… unless we think in terms of CP renewal?

Commented [JW12]: There is a statement on H&S induction paperwork. Is that sufficient?

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Agreements which they will be expected to sign before being given access to school systems (at KS1 it would be expected that parents/carers would sign on behalf of the pupils).
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the School's e-safety Policy covers their actions out of school, if related to their membership of the school
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Commented [JW13]: See my earlier comment

Staff are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Pupils should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school and know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident Management

In this school:

- A DSL will be informed of any online safety incidents involving safeguarding or child protection concerns. The DSL will record these issues in line with our child protection policy.
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively.
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible.
- we will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.
- we will ensure that online safety concerns are escalated and reported to relevant agencies.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated.
- Details of how we will respond to cyberbullying are set out in our anti-bullying policy.

Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated and will be responded to in line with existing policies, including anti-bullying and behaviour.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the headteacher will obtain advice through the Education Safeguarding Advisory Service (ESAS) and/or the Police.

Commented [JW14]: Added highlighted text

Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a child may be at risk of radicalisation online, action will be taken in line with our child protection policy.

4. Managing the ICT infrastructure

- **Internet access, security (virus protection) and filtering**

This school:

- Has the educational filtered secure broadband connectivity through Turn IT On;
- Uses the Turn IT On Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, web chat, sites of an illegal nature, etc. Pupil access to music download or shopping sites – except those approved for educational purposes at a regional, is managed;

Commented [JW15]: regional level(?)

- All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Ensures network health through use of Sophos anti-virus software (from Turn IT On);

- Uses Turn IT On approved systems including secured email to send personal data over the Internet and uses encrypted USBs where staff need to access personal level data off-site;
- Only unblocks other external sites for specific purposes eg Internet Literacy lessons;
- Works in partnership with Turn IT On to ensure any concerns about the system are communicated so that systems remain robust and protect pupils;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable;
- Ensures all staff and pupils have signed an acceptable use agreement form and understands that they must report any concerns;
- Requires staff to preview websites before use [where not previously viewed or cached]; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; eg *yahoo for kids, KidRex* or *ask for kids* , Google Safe Search.
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search, reminding children of appropriate actions in case of inappropriate content;
- Informs all users that Internet use is monitored;
- Informs staff and pupils that they must report any failure of the filtering systems directly to the *system administrator* or *Head teacher.* Our system administrator logs or escalates as appropriate to the Turn IT On Helpdesk as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through documentation, staff meetings and the teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities e.g. Police and/or LA safeguarding team.

Commented [JW16]: I question whether these are used?

- **Network management (user access, backup)**

This school

- Uses a combination of class and individual, audited log-ins for users;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Ensures the Systems Administrator / network manager is up-to-date with Bucks CC policies and requires the Technical Support Provider (TIO) to be up-to-date with Bucks CC policies;
- Storage of all data within the school will conform to the UK data protection requirements
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

Commented [JW17]: This section is largely beyond my experience to comment on

To ensure the network is used safely, this school:

- Ensures staff read and sign the school's AUP (Acceptable Use Agreement). Following this, they are set-up with Internet, email access and network access. Network access is through a unique, audited username and password;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- KS2 pupils are provided with an individual network log-in username. Year 6 are also expected to use a personal password;

- 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 as these have far less security restrictions and inappropriate use could damage files;
- Has set-up the network with shared work areas for pupils, one for staff and another for admin. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended. Staff are expected to lock their computers when not in use;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves. Users with access to secure data are timed out after 20 minutes and have to re-enter their password to re-enter the network;
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day to save energy;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities;
- Maintains equipment to ensure Health and Safety is followed e.g. projector filters cleaned; equipment installed and checked by approved suppliers/electrical engineers;
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role e.g. teachers access report writing module; SEN coordinator - SEN data;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files (done remotely through Turn It On);
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements (recovery data held with Turn It On);
- Uses CCTV systems set-up by Octagon and AVW Electrical Services;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Has firewalls and routers configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

Passwords policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

E-mail

This school

- Provides staff with an email account for their professional use (*@castlefield.bucks.sch.uk)* and makes clear personal email should be through a separate account;
- Uses email with content control with pupils.
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example office@castlefield.bucks.sch.uk. Class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public is available on request.
- 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.
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e-mails dangerous. We use a number of TIO-provided technologies to help protect users and systems in the school, including desktop anti-virus products, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.

Pupils:

- We use Google Mail with pupils and lock this down where appropriate using Google Mail domain settings.
- Pupils' e-mail accounts are intentionally 'anonymised' for their protection.
- Pupils are introduced to, and use e-mail as part of the Computing scheme of work.
- Pupils can only receive external mail from, and send external mail to, addresses if the Google Mail domain settings have been set to allow this.
- Pupils are taught about the safety and '*netiquette*' of using e-mail both in school and at home i.e. they are taught:
  - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
  - that an e-mail is a form of publishing where the message should be clear, short and concise;
  - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
  - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
  - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
  - that they should think carefully before sending any attachments;
  - embedding adverts is not allowed;
  - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
  - not to respond to malicious or threatening messages;
  - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
  - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
  - that forwarding 'chain' e-mail letters are not permitted.

- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff only use *@castlefield.bucks.sch.uk* e-mail systems for professional purposes
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems or encrypted data sticks
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':

  - the sending of multiple or large attachments should be limited, and is also restricted by the provider of the service being used;
  - the sending of chain letters is not permitted;
  - embedding adverts is not allowed;

School website

- The headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to teaching staff;
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the 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;
- The point of contact on the website is the school address, telephone number and we use a general email contact address, office@castlefield.bucks.sch.uk. Home information or individual e-mail identities will not be published;
- 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;
- We expect teachers using school approved blogs or wikis to password protect them and run from the school website.

Social networking

- See Social Networking Policy

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing

This school

- Only uses the TIO supported services for video conferencing activity;
- Only uses approved or checked webcam sites;
- Uses Skype as part of the interview process.

- All videoconferencing and/or webcam equipment will be switched off and disabled when not in use and will not be set to auto-answer.
- External IP addresses will not be made available to other sites.
- Videoconferencing contact details will not be posted publically.
- Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and pupil safety.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who the key contact(s) for key school information (the Information Asset Owners) are.
- We ensure staff know to whom they must report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record within the school's SIMS database.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Commented [JW18]: Does this cover Meet, Teams and Zoom?

Commented [JW19]: IS that the case?

Commented [JW20]: This needs doing

Technical Solutions

- Staff have secure areas on the network to store sensitive documents and photographs.
- We require staff to log-out of systems when leaving their computer.
- We use encrypted laptops are used by all staff and VPNs with remote access enable safe access to sensitive information on the school's network, without the need for flash drives.
- We use TIO for the creation of online user accounts for access to broadband services
- The on-site server is managed by DBS-checked staff, and is located in a lockable location.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.

6. Equipment and Digital Content

Personal mobile phones and mobile devices - General

- Mobile phones brought into school are entirely at the staff member, pupil's & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Staff members may use their phones during school break times. All visitors are requested to follow the same protocol as staff.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- Where there is a reasonable suspicion that a mobile or handheld device on the school premises may contain undesirable material, including those which promote pornography, violence or bullying, the School reserves the right to pass the information on to the police.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas/times within the school site under any circumstances e.g. changing rooms, classrooms when children are changing and toilets.
- Mobile phones should be switched off or on 'silent' mode unless they are being used as part of an approved and directed curriculum-based activity with consent from the headteacher.
- The Bluetooth or similar function of a mobile phone, e.g. AirDrop, should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Pupils' use of personal devices

- Pupils are not permitted to bring mobile phones or personally-owned devices to school unless authorisation has been obtained from the headteacher. On these occasions, phones brought into school, must be turned off (not placed on silent) and given to the teacher for storage. They must remain turned off and out of sight until the end of the day.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for the child's own safety.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place. Mobile phones and devices will be released to parents or carers.

Commented [JW21]: This is through the bitlocker login, isn't it? Does that need making explicit?

Commented [JW22]: Do we?

Commented [JW23]: Given pupil phones are collected in, locked away and returned at the end of the day, can we say we have no responsibility for pupil phones?

Commented [JW24]: Do staff know this?

- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone 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.

- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone.

- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Where necessary 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.

- Any unauthorised devices brought into school will be confiscated.

Staff use of personal devices

- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils without first seeking permission from the headteacher and will only use work-provided equipment for this purpose.

- Any permitted images or audio files of children taken in school on a personal device must be downloaded from the device and deleted in school before the end of the day, as this may compromise the safeguarding of children. Failure to do so may be met with disciplinary action. Staff are advised to 'show' a senior member of staff that they are deleting the content and to also clear their 'deleted photos/videos/audio clips' folder.

- Staff members may use their phones during school break times.

- 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 permission from the headteacher to use their phone outside their break times.

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

- In case of emergency during off-site activities, a member of staff should use their own device to contact the school office who will then make any further calls needed.

- If a member of staff is ever required to call anyone other than the school office for work related reasons, then they should hide their own mobile number (by inputting 141) for confidentiality purposes.

- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the headteacher.

- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video

In this school:

- 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 online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;

- Staff sign the school's Acceptable Use Agreement and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;

- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;

- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which

Commented [JW25]: Including smartwatches

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 public, personal information.

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

Asset disposal

Commented [JW26]: Beyond my experience.

- Details of all school-owned hardware will be recorded in a hardware inventory. (Asset Register)
- Details of all school-owned software will be recorded in a software inventory. (Turn It On)
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
- 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.

APPENDIX A

PUPILS' INTERNET CODE OF PRACTICE

- I will only use the Internet when supervised by a teacher or adult
- I will never tell anyone I meet on the Internet my home address, my telephone number, or my school's name, unless my teacher specifically gives me permission
- I will never send anyone my picture without permission from my teacher/parents/carer
- I will always log on to my computer using the correct password and I will log off when I have finished using the computer
- I will never arrange to meet anyone in person without first agreeing it with my parents/teachers/carer and get them to come along to the first meeting
- I will never hang around in an Internet chat room if someone says or writes something which makes me feel uncomfortable or worried, and I will always report to a teacher or parent
- I will not look for bad language or distasteful images while I am online and I will report bad language or distasteful images to a teacher if I come across them accidentally
- I will always be myself and will not pretend to be anyone or anything I am not
- I understand that my teacher and the Internet service provider can check the sites I have visited
- I understand that my teacher and the Internet service provider can check the sites and material relevant to my work in school and I will not be able to use the Internet if I deliberately look at unsuitable material

Pupil's signature ……..

Parent's signature …… Date ……..

<u>APPENDIX B</u> - Acceptable Use Agreement including photo/video permission (Parents)
Using images of children – Consent form for use by Castlefield School

To Name of the child's parent or guardian: _____

Name of child: _____

School: _____

Occasionally, we may take photographs of the children at our school. We may use these images in our schools prospectus or in other printed publications that we produce, as well as on our website. We may also make video or webcam recordings for school-to-school conferences, monitoring or other educational use.

Photographs or film footage by parents or guardians of their children at school events is permitted under an exemption in the Data protection Act 1998. There is also a journalistic exemption with regard to the media and occasionally pupil's images may appear in local or national newspapers, or on televised news programmes. Please indicate if you do not wish your child to appear in the media, if not we will try to keep your child out of the photographs.

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child. Please answer questions 1 to 4 below, then sign and date the form where shown.
Please return the completed form to the school as soon as possible.

	Please circle your answer
1. May we use your child's photograph in the school prospectus and other printed publications that we produce for promotional purposes?	**Yes / No**
2. May we use your child's image on the school's website and the school's social media?	**Yes / No**
3. May we record your child's image on video or webcam?	**Yes / No**
4. Are you happy for your child to appear in the media	**Yes / No**

Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies.

Please also note that the conditions for use of these photographs are on the back of this form.

I have read and understood the conditions of use on the back of this form.

Parent/guardian signature: _____ Date: _____

Name (in block capitals): _____

Conditions of use

1. This form is valid for five years from the date you sign it, or for the period of time your child attends this school. The consent will automatically expire after this time.
2. We will not re-use any photographs or recordings after your child leaves this school.
3. We will not use the personal details or full names (which means first name **and** surname) of any child or adult in a photographic image on video, on our website, in our school prospectus or in any of our other printed publications.
4. We will not include personal e-mail or postal addresses, or telephone or fax numbers on video, on our website, in our school prospectus or in other printed publications.
5. If we use photographs of individual pupils, we will not use the name of that child in the accompanying text or photo caption.
6. If we name a pupil in the text, we will not use a photograph of that child to accompany the article.
7. We may include pictures of pupils and teachers that have been drawn by the pupils.
8. We may use group or class photographs or footage with very general labels, such as “a science lesson” or “making Christmas decorations”.
9. We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.