Council

Meeting Date	24 September 2026
Title	Development of safeguarding guidance
Author(s)	Rosemary Flowers-Wanjie, Policy Lead
Executive Sponsor	Andrew Smith, Executive Director of Education, Registration & Regulatory Standards

Executive Summary

Following the standards of conduct, performance and ethics and guidance review (2022-24), we identified a need to develop standalone safeguarding guidance. Guidance on safeguarding currently resides within the guidance on confidentiality (Appendix B pages 16-18).

This paper provides a rationale for the development of standalone guidance on safeguarding for registrants. It also details the stakeholder engagement that informed the development of the safeguarding guidance, along with proposals to update safeguarding terminology in the standards of conduct, performance and ethics, guidance and across the HCPC website.

Action required	The Council is asked to consider and approve the proposal or recommendation. We seek the Council's approval to publish guidance on safeguarding for registrants and to make a minor consequential terminology change to the standards of conduct, performance and ethics.
Previous consideration	We have updated the Council on the progress of the safeguarding work in previous Chief Executive reports. The last update we gave was in November 2025. The paper was also considered by the Executive Leadership team (ELT) on 8 September 2026.
Next steps	Subject to the Council's approval we plan to publish the safeguarding guidance in quarter 3 2026-27. We will also make the minor consequential terminology change to the standards. The publication of the guidance and the changes to the standards will be supported by communication to

	stakeholders such as registrants, professional bodies and other relevant stakeholders.
Financial and resource implications	The costs of this project are incorporated into the financial year 2026-27 budget.
Associated strategic priority/priorities	Putting patients at the centre of smarter, preventative regulation Supporting healthcare workforce development through proportionate, agile regulation
Associated strategic risk(s)	SR01 - Delivery of Regulatory Requirements SR11 - Responding to Regulatory Change
Risk appetite	Regulation - measured Influence/leadership - seeks
Communication and engagement	To inform the development of the guidance, we engaged with service users, carers and parents who have experiences of safeguarding processes. We also received feedback on the guidance from professional bodies during a Professional Body's Forum in March 2026.
Equality, diversity and inclusion (EDI) impact and Welsh language standards	The guidance supports the HCPC's EDI objectives by reinforcing inclusive, fair and person-centred safeguarding practice, helping registrants recognise and respond appropriately to the needs of people who may be at greater risk of harm or disadvantage. It also supports the consistent application of existing HCPC standards and expectations relating to equality, diversity and inclusion, rather than introducing new EDI requirements. The guidance is not expected to have any impact on the HCPC's Welsh language commitments, as it does not affect opportunities to use Welsh or the principle of treating Welsh and English equally. If the guidance is made available in Welsh, it may have a positive impact by improving accessibility for Welsh-speaking stakeholders.
Other impact assessments	None
Reason for consideration in the private session of the meeting (if applicable)	Not applicable

Development of safeguarding guidance

1. Background

1.1. Following the standards of conduct, performance and ethics (SCPEs) and guidance review (2022-24), we identified a need to develop standalone safeguarding guidance. Guidance on safeguarding currently resides within the Guidance on Confidentiality (Appendix B p.16-18). This section is limited to safeguarding being a matter of identifying when it is appropriate for a registrant to disclose service user information. Subject to Council approval of the standalone safeguarding guidance, we will update the guidance on confidentiality, removing detail on safeguarding, to avoid duplication.

1.2. Registrants' safeguarding responsibilities are set out in Standard 7 of the SCPEs and are much broader than information sharing. Safeguarding is about protecting the health, well-being and human rights of children, and adults at risk, so that they can live free from harm, abuse and neglect.

1.3. Accordingly, safeguarding can encompass identifying risks and indicators of harm, taking action to prevent harm, escalating concerns, supporting a culture of speaking up and responding to concerns raised by others and prioritising service user welfare over organisational or professional loyalties. Standalone guidance on safeguarding enables us to set out our expectations of registrants in a clear, detailed and accessible way.

1.4. During stakeholder engagement for the SCPEs review, the suggestion of standalone safeguarding guidance was also mentioned by registrants in webinars and by a regional safeguarding lead.

2. Guidance

2.1. The safeguarding guidance (Appendix A) includes rewritten content from the confidentiality guidance along with further guidance on the meaning of safeguarding in health and care practice. We have also included signposting to relevant external material about safeguarding and the processes that registrants are expected to follow. The new guidance includes the following sections:

- What safeguarding is and key principles
- Legal duties and relevant national frameworks
- Expectations under SCPE Standard 7 on reporting and escalation
- Information sharing and confidentiality
- Working with families, carers and multi-agency partners
- Links to legislation, national policy and additional resources

3. Stakeholder engagement

3.1. To inform the development of the guidance, we commissioned the Patients' Association to undertake service user engagement. This engagement focused on two pieces of work: a focus group involving 10 adult service users and carers with experience of safeguarding in health and care settings, and a series of case study interviews with children and their parents or guardians who had been involved in safeguarding processes.

3.2. Participants represented a range of backgrounds, health conditions, UK geographic locations and experience from across the health and care system. The engagement was intended to ensure that the perspectives of those who may be directly affected by safeguarding activity were considered during the development of the guidance.

3.3. Feedback from participants highlighted several common themes from their experiences of safeguarding. These included a lack of clear communication about safeguarding processes, feelings of fear and uncertainty when safeguarding concerns were raised, limited involvement in decision-making, and a perceived lack of support during and after safeguarding interventions. Participants also emphasised the importance of person-centred approaches, clear and accessible information, empathy and kindness from professionals, and greater understanding of how safeguarding decisions are made.

3.4. The draft guidance was generally welcomed by participants, who considered it a useful resource for registrants. However, they identified opportunities to strengthen certain areas, including:

- clearer explanations of safeguarding processes and responsibilities;
- greater emphasis on involving service users, families and carers where appropriate;
- signposting to sources of support;
- clearer explanation of how safeguarding operates within wider multi-agency arrangements; and
- improved accessibility of information.

3.5. We also engaged with professional bodies through the Professional Bodies Forum and requested feedback on the draft guidance. The guidance was positively received and noted as a beneficial for registrants, along with learners and future HCPC registrants. It was also agreed that the existence of standalone guidance makes it easier for registrants to find the information they need about safeguarding.

3.6. We also received helpful comments on how to further improve the guidance. This included:

- advice to ensure the terminology used was up to date, for example the use of 'adult at risk' rather than "'vulnerable adult' (see further discussion below); and

- suggested resources and legislation to include for example, the Mental Health Act 2025.

3.7. These comments were gratefully noted and have since been reflected in our final draft.

4. Terminology updates to Standards of conduct, performance and ethics

4.1. As part of this work, we heard suggestions from professional bodies to replace the term ‘vulnerable adult’ with ‘adult at risk’ within the guidance. We have reflected this in the final version of the guidance and recommend duplicating this across the relevant parts of the HCPC website, standards and guidance documents.

4.2. Regarding the standards of conduct, performance and ethics, the terminology change we propose would be reflected in Standard 7.3:

- Current wording: *You must take appropriate action if you have concerns about the safety or well-being of children or vulnerable adults.*
- Proposed revised language: *You must take appropriate action if you have concerns about the safety or well-being of children or adults who experience or are at risk of abuse or neglect.*

4.3. This change is not substantive, and it does not impact our expectations of registrants regarding safeguarding in practice. The change will bring the language of the standards into alignment with current usage. Due to the nature of the change, we do not propose to consult on the revised wording of this standard. However, should the proposed revision be approved, we would ensure that the change is clearly communicated to registrants, professional bodies and other relevant stakeholders.

4.4. The term ‘adult at risk’ is increasingly recognised and used across safeguarding legislation, policy and professional practice. This shift is reflected in legislation and statutory guidance across the UK, including the Social Services and Well-being (Wales) Act 2014, which defines an adult at risk, and the Adult Support and Protection (Scotland) Act 2007, which refers to adults at risk.

4.5. The Care Act 2014 is the principal adult safeguarding legislation in England. It does not use the term "vulnerable adult" as a statutory definition. Instead, it focuses on adults with care and support needs who are experiencing, or are at risk of, abuse or neglect. This reflects a shift away from defining people by vulnerability and towards identifying and responding to risk.

4.6. The term ‘adult at risk’ focuses on the circumstances that may place an individual at risk of harm rather than implying an inherent or permanent characteristic of vulnerability. This person-centred and strengths-based approach aligns with contemporary safeguarding principles and helps avoid language that could be perceived as labelling or stigmatising individuals.

4.7. Updating our terminology would promote consistency with current safeguarding practice and ensure that HCPC publications reflect modern, inclusive language.

5. Next steps

5.1. We are seeking Council approval to publish the guidance on safeguarding for registrants and to make a terminology change to the Standard 7.3 of the Standards of conduct, performance and ethics.

Guidance on safeguarding

Contents

Introduction

About this document

This document provides guidance on registrant responsibilities to effectively safeguard children, and adults who are experiencing, or may be at risk from, abuse or neglect. Registrants have a duty to ensure the safety of children and adults at risk as set out in our standards of conduct, performance and ethics. All safeguarding concerns must be dealt with and escalated accordingly.

We have written this guidance for our registrants however, it may also interest potential registrants, learners, employers and other people who want to know how we expect professionals to approach safeguarding. It is not designed to replace local procedures. However, it is meant to help registrants make informed and reasonable decisions relating to issues of public safety, service user protection and confidentiality, in line with our standards.

This guidance supports our Standards of Conduct, Performance and Ethics and applies UK-wide. It has been developed to align with the relevant legislation in England, Scotland, Wales and Northern Ireland.

Some professional bodies publish safeguarding advice and guidelines to support their members to meet their obligations. If you are employed, your employer may also have relevant policies or guidance that apply to you.

How this document is structured

This document is divided into three sections.

- Section 1 provides a definition of safeguarding and some important information about safeguarding in the UK.
- Section 2 outlines what our standards say about safeguarding and what we expect of registrants.
- Section 3 contains links to further resources.
- Section 4 sets out how you can contact us for further information.

Throughout the document, you may see sections like this. These text boxes provide extra definitions for some of the phrases we are using.

Language

Throughout this document:

- ‘we’ and ‘us’ refers to the Health and Care Professions Council (HCPC);
- ‘registrant’ refers to a professional on our register;
- ‘you’ or ‘your’ refers to a registrant and;
- ‘service user’ refers to anyone who uses or is affected by the services of registrants, for example, patients or clients

About us

We are the Health and Care Professions Council. Our statutory role is to protect the public by regulating healthcare professionals in the UK. To do this, we keep a register of professionals who are required to meet our standards for their professional skills, knowledge and behaviour. Individuals on our Register are called ‘registrants’. We currently regulate 15 professions; you can find out which professions we regulate here.

We promote high quality professional practice, regulating over 360,000 registrants by:

- setting standards for professionals' education and training and practice;
- approving education programmes which professionals must complete to register with us;
- keeping a register of professionals, known as 'registrants', who meet our standards;
- acting if professionals on our Register do not meet our standards; and
- stopping unregistered practitioners from using protected professional titles.

HCPC and safeguarding

As a regulator and a public authority, HCPC has a responsibility to play our part effectively in safeguarding children and adults at risk from harm. While we do not work specifically with children or adults at risk, we may engage with them. This could include members of the public (for example, complainants) or HCPC registrants that encounter us over the course of our activities. In line with our values, we strive to treat with care and compassion, all those people we work and engage with, both as a regulator and an employer.

We have set out our safeguarding responsibilities in our Safeguarding Policy, so that our staff and partners are aware of their safeguarding obligations, and to ensure that any safeguarding concerns are dealt with and escalated appropriately.

About the standards

We set standards of conduct, performance and ethics, which set out how we expect registrants to behave. We use the standards:

- to help us to make decisions about the character of professionals who apply to our Register;
- if someone raises a concern about a registrant’s practice; and
- when things go wrong, they help us to decide whether it is necessary to act.

As a registrant, you must make sure you are familiar with the standards and that you continue to always meet them.

Our current standards of conduct performance and ethics can be found at the HCPC website: standards of conduct, performance and ethics | (hcpc-uk.org).

Section 1: Safeguarding in health and care

What is safeguarding

What is safeguarding?

Safeguarding is about protecting the health, well-being and human rights of children and adults, so that they are able to live free from harm, abuse and neglect[1].

When a registrant comes into contact with children, or adults at risk, they have a role to play in identifying concerns, sharing information and taking steps to help keep them safe.

Who is a child?

A child is a person aged under 18 years of age. The terms 'child' and 'children' are used in this guidance to refer to children and young people who have not reached their 18th birthday.

Safeguarding children is about ensuring their safety, which requires:

- providing help and support to meet the needs of children as soon as problems emerge
- protecting children from maltreatment, whether that is within or outside the home, including online
- preventing the impairment of children's mental and physical health or development
- ensuring that children grow up in circumstances consistent with the provision of safe and effective care
- taking action to enable all children to have the best outcomes[2].

Child protection is part of safeguarding and promoting the welfare of children and is defined for the purpose of this guidance as activity that is undertaken to protect specific children who are suspected to be suffering, or likely to suffer, significant harm. This includes harm that occurs inside or outside the home, including online.

Who is an adult at risk?

An adult at risk is any person who is aged 18 or over and at risk of abuse or neglect and may have additional needs for care and support.

Safeguarding adults includes, where appropriate, having regard to their views, wishes, feelings and beliefs when deciding on any action. It involves recognising that adults sometimes have complex interpersonal relationships and may be ambivalent, unclear or unrealistic about their personal circumstances[3].

[1] NHS England » About NHS England Safeguarding and **Care Quality Commission (CQC). *Safeguarding people*.** https://www.cqc.org.uk/about-us/how-we-do-our-job/safeguarding-people

[2] Working together to safeguard children 2023: statutory guidance

[3] Care Act 2014: Care and support statutory guidance (England). For Wales, see Social Service and Well-being (Wales) Act 2014: Working Together to safeguard people.

Safeguarding concerns can take many different forms, including:

- Physical, psychological or sexual abuse.
- Financial or material abuse.
- Neglect and acts of omission.
- Discriminatory abuse, such as racist or sexist remarks.

Should a concern arise for a child or adult at risk, this concern should be reported as soon as possible to the relevant emergency services, such as the police and /or local authority safeguarding children or adults at risk team, as appropriate. Always follow local procedures.

Effective safeguarding means practitioners should understand and be sensitive to factors, including economic and social circumstances and ethnicity, which can impact children and families' lives.

Practising safeguarding: top tips

- Use supportive, non-accusatory language.
- Explain safeguarding processes clearly to patients and families.
- Provide reassurance that safeguarding does not imply blame.

Safeguarding and the law

You have a professional and legal responsibility to raise concerns about the safety of children and adults at risk. It is a professional responsibility because our standards are there to protect the public and say that you must raise concerns about the safety of children and adults at risk (Standard 7.3). Safeguarding issues can affect your registration.

It is a legal responsibility because of the principles set by law, which say that professionals have a duty to protect and ensure the safety of children and adults at risk. The law also sets out when you can disclose information to meet safeguarding responsibilities.

This guidance draws on relevant laws that affect health and care professionals and their service users. You are not expected to be an expert on the law, but you must keep up to date with and meet your legal responsibilities. Where helpful, we have referred directly to specific legislation which covers issues related to safeguarding.

Apart from the law, there is a large amount of guidance produced by other organisations, such as professional bodies, which may apply to you. If you are employed, your employer is also likely to have policies about safeguarding. You should keep up to date with and follow any guidance or policies that are relevant to your practice.

We expect our registrants to be autonomous and professional. You should be aware of their local policies relating to safeguarding. This may include:

- employer child protection policy (which may include the policy and procedures to deal with child-on-child abuse)
- employer behaviour policy (which may include measures to prevent bullying, including cyberbullying, prejudice-based and discriminatory bullying).
- employer staff behaviour policy (which may include low-level concerns, allegations against staff and whistleblowing)

- safeguarding response to children who are absent from education, particularly on repeat occasions and/or prolonged periods
- role of the designated safeguarding lead (including the identity of the designated safeguarding lead and any deputies)[4]

The Department for Education (DfE) have set out that a child-centred and multi-agency approach is necessary to ensure effective safeguarding. This applies to all agencies and professionals involved in safeguarding and protecting children. Specifically, those in health services, the police, local authorities, probation services, youth offending services, education providers and childcare settings, and voluntary and third sector organisations.

Safeguarding with others: top tips

HCPC guidance complements local authority and statutory safeguarding frameworks. Registrants should collaborate with designated safeguarding leads and other agencies as required.

There are specific safeguarding partners in a local authority (the local authority, an integrated care board and the chief officer of the police), as set out under the Children Act 2004 (amended by the Children and Social Work Act, 2017). They have a statutory duty to work together to safeguard and promote the welfare of the local children in their area and set the strategic direction of safeguarding.

Each partner has a Lead Safeguarding Partner who is responsible for discharging their own statutory and legislative duties to safeguard and promote the welfare of children. These are; Chief Executives of Local Authorities, Chief Executives of the integrated care boards, and Chief Officers of police forces.

Depending upon your place of work there may also be a designated safeguarding lead. These designated health practitioners are an important source of safeguarding advice and expertise. Where you are unsure of your obligations, you may which to seek the advice of the designated practitioner within your organisation or local area.

Key principles

This guidance cannot cover every situation where you may need to report concerns about the safety of a child or adult at risk. However, you should keep the following principles in mind. The guidance that follows builds on these principles to explain more.

You should:

- Seek to empower children and adults at risk,
    - Support and encourage adults at risk to make their own decisions and give informed consent.
    - Ensure children's wishes are sought, heard and responded to and work in partnership with families
- Treat children and adults at risk with dignity and respect, delivering person-centred care that ensures they are safe on their terms.

[4] [4] Working together to safeguard children 2023: statutory guidance

- Take action to prevent harm and put mechanisms in place so that harm does not recur. This may include:
    - seeking medical attention if needed
    - recording what you have found
    - seeking advice from a safeguarding lead
    - checking for other indicators
    - discussing with a manager or supervisor
    - monitoring the situation to see if it improves
- Build trust with the families and carers:
    - signpost patients and families to relevant support services, including mental health and advocacy organisations. This helps reduce emotional burden.
- After taking these steps, if the situation does not improve, raise your level of concern to 'abuse or neglect is suspected'.
- Be proportionate in your response ensuring that you decide on the least intrusive response. An individual's wishes and circumstances should be considered.
- Protect individuals in greatest need, delivering support to them and representing those who may not be able to do so themselves.
- Partner with other organisations involved in the safeguarding of children and adults at risk when you have a concern about safeguarding.
- You must be accountable, open and honest when you are safeguarding a child or adult at risk.[5]

Maintaining your safeguarding skills: top tips

You may wish to undertake safeguarding training that includes:

- Communication skills
- Empathy and kindness
- Awareness of power imbalances

[5] These principles follow those set out by the UK government in Revisiting safeguarding practice - GOV.UK and Working together to safeguard children 2023: statutory guidance

Section 2: Safeguarding in our standards

Raising concerns and reporting requirements

Our Standards of conduct, performance and ethics set out in Standard 7 that you must report concerns about safety.

What is reporting a concern about safety?

When we refer to 'reporting concerns', we mean ensuring that where you have a concern about safety, your concern is escalated appropriately to resolve the concern.

Our standards of conduct, performance and ethics say that:

Standards 7.3: 'You must take appropriate action if you have concerns about the safety or well-being of children or adults who experience or are at risk of abuse or neglect.'

In these situations, the following apply.

− If you are employed, you should follow your organisation's local safeguarding policies and procedures for raising a concern. This may include reporting the matter to your safeguarding lead, manager, local authority safeguarding team, or the police, depending on the circumstances.

− If you are self-employed, you should take appropriate safeguarding action in line with local procedures. This may include reporting the matter to the local authority safeguarding team, the police, a commissioning organisation, or a regulator. Where appropriate, concerns should also be referred to the Disclosure and Barring Service (DBS), or in Scotland, Disclosure Scotland.

You are expected to disclose information with partner organisations where necessary. This is supported by UK data sharing legislation[6] and does not interfere with your responsibility to maintain confidentiality that is set out in our standards of conduct performance and ethics.

Disclosing information

Making a disclosure is when identifiable information is revealed, released or passed on from one person to another.

When raising a concern, it is important that you:

- Keep a record of any disclosures that you make and the reasons for the disclosure.
- Only provide the information relevant to the concern. Provide anonymised or partly anonymised information where you can.

Our standards of conduct, performance and ethics (Standard 5.2) say that:

'You must only disclose confidential information if:

[6] https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

- you have permission;
- the law allows this;
- it is in the service user's best interests; or
- it is in the public interest, such as if it is necessary to protect public safety or prevent harm to other people.'

You may be required by safeguarding partners to provide them, or any relevant agency for the area, a reviewer or another person, or organisation, with specified information to enable and assist the lead safeguarding partners to safeguard and promote the welfare of children in their area. This includes local and national child safeguarding practice reviews. You must comply with this request[7].

Sometimes, we may request information from you as part of a fitness to practise investigation.

Where you are raising a concern about a child, or an adult and/or their family member and need to share identifiable information, it is good practice to tell them that you are going to do so and try to get their consent. In some circumstances – for example, in the public interest – identifiable data can be disclosed without consent.

Disclosing information in the public interest might be in circumstances where disclosing the information is necessary to prevent a serious crime or serious harm to other people. You can find out whether it is in the public interest to disclose information by considering the possible risk of harm to other people if you do not pass it on, compared with the possible consequences if you do. This includes taking account of how disclosing the information could affect the care, treatment or other services you provide to the service user.

You should carefully consider whether it is in the public interest to disclose the information. If you are unsure, speak to your manager or employer (if you have one), or your trade union or professional body. You may also want to get legal advice. You need to be able to justify a decision to disclose information in the public interest (or a decision not to disclose information) so it is important that you keep clear records.

In some circumstances it may not be possible to get consent from a service user to share information. For example, in some emergency situations, they may be unable to communicate or give consent because they are very unwell or unconscious. In other circumstances, they may not have capacity to give consent.

Working in partnership with parents/carers

You should work in partnership with parents and carers as far as possible. You should follow the principles of the Children Acts 1989 and 2004. These Acts make clear that the welfare of children is paramount and that they are best looked after within their families, with their parents playing a full part in their lives, unless compulsory intervention in family life is necessary.

If you are unsure about disclosing information, for example if you do not think the information requested is relevant, you should contact the person who has asked you for the information

[7] https://www.legislation.gov.uk/ukpga/2004/31/section/16H

so they can explain their request. You may also wish to seek legal advice or get advice from a trade union or a professional body. For more information about confidentiality and consent, see our Guidance on confidentiality.

Our standards of conduct, performance and ethics (Standard 7.5) say that:

‘You must follow up concerns you have reported and, if necessary, escalate them.

It is important that where you have raised a concern, you continue to follow up that concern until it is resolved.

Our standards of conduct, performance and ethics (Standard 7.6) say that:

‘You must acknowledge and act on concerns raised to you, investigating, escalating or dealing with those concerns where it is appropriate for you to do so’.

You may have specified safeguarding duties set out by your employer. It is important that if this applies to you, you have undertaken the appropriate safeguarding training relevant to your role. You must also understand any relevant policies or legislation that outline your obligations. If you are the recipient of any concerns about the safety of children or adults at risk, you must investigate, escalate or deal with them.

You can find further information about your obligations on our website, including our Standards of conduct, performance and ethics and other relevant guidance.

Section 3: Resources and other guidance

The below resources are some external sources of information related to safeguarding. There may be further sources relevant to your practice, provided by your employer or professional body.

UK government legislation

Children and Families Act 2014
Children Act 1989 and Children Act 2004
Domestic Abuse Act 2021
Prevent Duty 2023
Female Genital Mutilation Act 2003
Modern Slavery Act 2015
Mental Health Act 2007
Mental Capacity Act 2005 and Mental Capacity (Amendment) Act 2019
Data Protection Act 2018

UK government guidance

Working together to safeguard children 2023: statutory guidance
Keeping children safe in education 2024
DfE non statutory information sharing advice for practitioners providing safeguarding services for children, young people, parents and carers
Safeguarding Adults: The role of health services - GOV.UK
Revisiting safeguarding practice - GOV.UK
Guidance for health professionals on domestic violence - GOV.UK
Promoting the Health of Looked After Children Statutory Guidance 2015
National Guidance for Child Protection in Scotland 2021 - updated 2023 - gov.scot
Safeguarding guidance | GOV.WALES
Working together to safeguard people: code of safeguarding practice | GOV.WALES
Adult Safeguarding: Prevention and Protection in Partnership | Department of Health

NHS guidance

NHS England » Safeguarding children, young people and adults at risk in the NHS: Safeguarding accountability and assurance framework
NHS Constitution and Values (updated Jan 2021)

Other sources of guidance

We recognise the valuable role professional bodies play in representing and promoting the interests of their members. This often includes guidance and advice about good practice which can help you meet the standards that we set.

More information

You can download copies of our standards documents and other publications from our website at www.hcpc-uk.org

To request this document in Welsh or an alternative format, email publications@hcpc-uk.org.

Glossary

You may not be familiar with some of the terms we use throughout this document, so we have explained them below.

As an accountable health and care professional, you will be responsible for the decisions you make and you may also be asked to justify them.

Autonomous

As an autonomous health and care professional, you make your own decisions based on your own professional judgement.

Child

A person aged under 18 years of age. The terms 'child' and 'children' are used in this guidance to refer to children and young people who have not reached their 18th birthday.

Disclose, disclosure

When information is revealed, released or passed on from one person to another.

Fitness to practice

A professional is fit to practise if they have the training, skills, knowledge, character and health to do their job safely and effectively. We can take action if we have concerns about a registrant's fitness to practise.

Identifiable information

Any information that might identify a service user, for example their name, address or details of their health condition, treatment or care.

Implied consent

When a service user is aware of the possibilities for sharing information and their right to refuse this, but does not object.

Informed consent

When a service user has enough information to make a decision about whether they give their permission for information to be shared with other people.

Lead Safeguarding Partner

The person responsible for discharging the statutory and legislative duties of Local Safeguarding Partners to safeguard and promote the welfare of children. These are; Chief Executives of Local Authorities, Chief Executives of the integrated care boards, and Chief Officers of police forces.

Local Safeguarding Partner

Bodies within a local authority (the local authority, an integrated care board and the chief officer of the police), as set out under the Children Act 2004 (amended by the Children and Social Work Act, 2017). They have a statutory duty to work together to safeguard and

promote the welfare of the local children in their area and set the strategic direction of safeguarding.

Professional bodies

Organisations which promote or represent members of a profession. They may also provide guidance and advice, produce curriculum frameworks, oversee post-registration education and training, and run continuing professional development (CPD) programmes.

Public interest

Disclosures of information are made in the 'public interest' when it is necessary to prevent a serious threat to public health, national security, the life of the person concerned or another person, or to prevent or detect serious crime.

Register

A published list of health and care professionals who meet our standards. The Register is available on our website at www.hcpc-uk.org

Registrant

A health and care professional who appears on our Register and meets our standards.

Regulator

An organisation that protects the public by making sure people or organisations keep to certain laws or requirements.

Safeguarding

Protecting the health, well-being and human rights of children and adults, so that they are able to live free from harm, abuse and neglect.

Service user

Anyone who uses or is affected by the services of a registrant. This includes patients and clients.

Standards of conduct, performance and ethics

Standards of behaviour that we expect from health and care professionals who are registered with us.

Statutory powers

Certain organisations, such as regulators, have powers under legislation. This sometimes includes the power to ask for information from people.

Adult at risk

Any person who is aged 18 or over and at risk of abuse or neglect and has additional needs for care and support.

hcpc health & care professions council

Information for registrants

Confidentiality – guidance for registrants

Contents

Section 1:
About this document

This document provides guidance on some of the issues relating to how health and care professionals handle information about service users. We have written it mainly for our registrants, but it might also be helpful to potential registrants, employers and other people who want to know how we expect professionals to approach issues of confidentiality.

This document is not designed to replace local procedures and is not meant to cover every situation where problems can come up. However, it is meant to help you make informed and reasonable decisions relating to issues of confidentiality, in line with our standards.

If you have any questions after reading this document, please see the 'More information' section on page 20. We also explain some of the terms and phrases we use throughout this document in the glossary on page 21.

Language

In most of this guidance, when we refer to 'service users' we mean patients, clients and other people who are directly affected by the care, treatment or other services that registrants provide. The broad principles set out in this guidance also apply to registrants who provide services to organisations rather than individuals.

In this document, 'you' means a registrant and 'we' and 'our' refers to the Health and Care Professions Council.

Section 2:
Key principles

This guidance cannot cover every situation where problems or challenges about confidentiality might come up. However, you should keep the following principles in mind when handling information. The guidance that follows builds on these principles to explain more.

You should:

– take all reasonable steps to keep information about service users safe;
– make sure you have the service user's consent if you are passing on their information (unless there are good reasons not to, for example, it is necessary to protect public safety or prevent harm to other people);
– get express consent, in writing, if you are using identifiable information for reasons which are not related to providing care, treatment or other services for them;
– only disclose identifiable information if it is necessary, and, when it is, only disclose the minimum amount necessary;
– tell service users when you have disclosed their information (if this is practical and possible);
– keep appropriate records of disclosure;
– keep up to date with relevant law and good practice;
– if appropriate, ask for advice from colleagues, professional bodies, unions, legal professionals or us; and
– make your own informed decisions about disclosure and be able to justify them.

Section 3:
About us

We are the Health and Care Professions Council (HCPC). We are a regulator and our main aim is to protect the public. To do this, we keep a register of professionals who meet our standards for their training, professional skills, behaviour and health.

Health and care professionals on our Register are called 'registrants'. If registrants do not meet our standards, we can take action against them. In serious cases, this may include removing them from the Register so that they can no longer practise.

Our registrants work in a variety of different settings and with a variety of different people. In this document, we refer to those who use or who are affected by the services of our registrants as 'service users'.

Who do we regulate?
We currently regulate the following professions.

– Arts therapists
– Biomedical scientists
– Chiropodists / podiatrists
– Clinical scientists
– Dietitians
– Hearing aid dispensers
– Occupational therapists
– Operating department practitioners
– Orthoptists
– Paramedics
– Physiotherapists
– Practitioner psychologists
– Prosthetists / orthotists
– Radiographers
– Speech and language therapists

Section 4: Introduction

Confidentiality means protecting personal information. This information might include details of a service user's lifestyle, family, health or care needs which they want to be kept private.

Service users expect the health and care professionals who are involved in their care or treatment, or have access to information about them, to protect their confidentiality at all times. Breaking confidentiality can affect the care or services you provide, as service users will be less likely to provide the information you need to care for them. Doing this may also affect the public's confidence in all health and care professionals.

This document builds on the principles outlined in section two and provides extra guidance about some of the issues which come up about confidentiality. It builds on the expectations of health and care professionals outlined in our standards of conduct, performance and ethics.

Our standards of conduct, performance and ethics

The following standards of conduct, performance and ethics describe the professional behaviour we expect from you. You must:

1. promote and protect the interests of service users and carers;
2. communicate appropriately and effectively;
3. work within the limits of your knowledge and skills;
4. delegate appropriately;
5. respect confidentiality;
6. manage risk;
7. report concerns about safety;
8. be open when things go wrong;
9. be honest and trustworthy; and
10. keep records of your work.

You can download copies of these standards from our website, or you can ask us to send you a copy. Please see the section 'More information' on page 20.

As our registrants work in a variety of settings and roles, we have written our standards so that they are relevant, as far as possible, to all registrants and all professions. We have also written them in a way that means they can take account of any changes in the law, technology or working practices.

Our standards are flexible enough to allow registrants and employers to take account of local circumstances – such as availability of resources – to develop ways of working that are practical, effective and meet the needs of service users.

We have written this document to help you meet our standards. However, there is often more than one way to do this. As a health and care professional, you need to make your own decisions (based on your own judgement) about the best way to meet our standards, taking account of your own practice and the needs of your service users. If someone raises concerns about your practice, we will take account of any steps you have taken, including following this guidance, when we decide whether you have met our standards.

Section 4: Introduction

Confidentiality and the law

You have a professional and legal responsibility to respect and protect the confidentiality of service users at all times.

It is a professional responsibility because our standards are there to protect the public and say that you should protect the confidentiality of service users at all times. Confidentiality issues can affect your registration.

It is a legal responsibility because of the principles set by law, which say that professionals have a duty to protect the confidentiality of the people they have a professional relationship with. The law also says how you should keep, handle and disclose information.

This guidance draws on relevant laws that affect health and care professionals and their service users. You are not expected to be an expert on the law, but you must keep up to date with and meet your legal responsibilities. Where helpful, we have referred directly to specific legislation which covers issues related to handling information, consent and capacity (see section 7 for more information about these).

Apart from the law, there is a large amount of guidance produced by other organisations, such as professional bodies, which may apply to you. If you are employed, your employer is also likely to have policies about confidentiality and sharing information. You should keep up to date with and follow any guidance or policies that are relevant to your practice.

Accessing and using information

When we refer to 'using' information, we mean any way information is handled. This includes accessing information, as well as disclosing information to third parties and using information in research or teaching.

This guidance focuses mainly on disclosing or sharing information with other professionals or third parties. However, accessing information (including care records) without good reason, permission or authorisation is considered to be breaking confidentiality, even if you do not then share the information with a third party. You should be sure that you have a legitimate reason for accessing information about service users, for example where you need it to provide care, treatment or other services. For other reasons you are likely to need specific permission from the service user.

Section 5:
What information is confidential?

Information about a service user can be ‘identifiable’ or ‘anonymised’. By identifiable information we mean any information you hold about a service user that could identify them. You must treat this information as confidential.

Identifiable information can include:

– personal details, such as names and addresses;
– information about a service user’s health, treatment or care that could identify them;
– photos, videos or other images; and
– other information that a service user, family member or carer shares with you that is not strictly related to the care, treatment or other services you provide.

Anonymised information is information about a service user that has had all identifiable information removed from it and where there is little or no risk of a service user being identified from the information available. You may be able to share anonymised information more openly in some circumstances. However, you should always consider carefully what you are sharing and who you are sharing it with.

Section 6:
Keeping information safe

What our standards say

Our standards of conduct, performance and ethics say that:

'You must treat information about service users as confidential' (5.1)

and

'You must keep records secure by protecting them from loss, damage or inappropriate access.' (10.3)

This means that you need to take all reasonable steps to protect information about service users. By 'reasonable steps', we mean that you need to take sensible, practical measures to make sure that you keep the information safe.

For example, you could store paper records in a lockable cabinet or room. If you run your own practice, you could develop a clear policy for your practice and provide training for your members of staff. Or, you might make sure that you avoid having conversations about service users in public areas where other people might be able to hear.

If you are employed by an organisation, your employer will normally have policies and guidelines on how you should store, handle and share information. In most circumstances, following these policies will allow you to meet our standards comfortably. However, you still need to think about your own practice to make sure that you are protecting confidentiality at all times.

As a responsible professional, it is important that you take action if you become aware that information about a service user has been lost, damaged or inappropriately accessed, or if there might be a risk of this happening. You should tell your employer (if you have one) and take steps to try to make sure that the problem does not happen again.

The General Data Protection Regulation (GDPR), supported by the Data Protection Act 2018 (DPA) governs how personal data (information), including service user records, should be handled. It outlines a number of data-protection principles. You can find more information in annex A at the back of this document and on the Information Commissioner's Office website.

Electronic records

Health and care records are increasingly being held electronically, rather than on paper. We do not provide any specific guidelines about the types or features of computer-based systems which registrants should use.

This is partly because technology changes quickly and we would not want to prevent you from using new technologies. It is also because the type of electronic record system you use will depend on your practice, the type of setting you work in and other factors.

If you are employed, you should follow your employer's policies and procedures for electronic record-keeping and keeping information secure.

If you are self-employed and need to set your own policies and procedures, you must make sure that you continue to meet our standards. This means making sure you keep electronic records secure and that they can only be accessed by the appropriate people. You should have an effective system in place for restricting access to the records – for example, personal logins and effective passwords.

Section 7:
Consent and confidentiality

Identifiable information is disclosed for a number of reasons. It can happen when you refer a service user to another health and care professional or when a service user asks for information to be given to a third party.

It is important that you get the service user's permission, or 'consent', before you share or disclose their information or use it for reasons which are not related to the care or services you provide for them. There are some exceptions to this and we cover these later in this document.

What our standards say

Our standards of conduct, performance and ethics say that:

'You must only disclose confidential information if:

– you have permission;
– the law allows this;
– it is in the service user's best interests; or
– it is in the public interest, such as if it is necessary to protect public safety or prevent harm to other people.' (5.2)

What is consent?

Consent, for the purposes of confidentiality, means that the service user understands and does not object to:

– the information being disclosed or shared;
– the reason for the disclosure;
– the people or organisations the information will be shared with; and
– how the information will be used.

For consent to be valid, it must be **voluntary** and **informed**, and the person giving consent must have the **capacity** to make the decision.

– By 'voluntary', we mean that the person makes the decision freely and without being persuaded or pressurised by professionals, family, friends or others.
– By 'informed', we mean that the service user has enough information to make a decision about whether they give their permission for their information to be shared with other people. (This is sometimes called 'informed consent'.) Service users should be fully aware of why you need to share any information about them, how you will do so, who you will be sharing the information with and how that information will be used. You should also tell them how not giving their permission is likely to affect the care, treatment or services they receive.
– By 'capacity' we mean a service user's ability to use and understand information to make a decision and to tell you that decision. We discuss capacity in more detail below.

There are two types of consent for the purposes of confidentiality – **express consent** and **implied consent**.

– Express consent

This is where you are given specific permission to do something. You need to get express consent if you are using identifiable information for reasons which are not related to the care, treatment or other services you provide for the service user, or in a way which they would not reasonably expect. It is also important to get express consent if a service user has previously objected to you sharing their information with other people. Express consent can be spoken or written.

If the service user has given you their express consent verbally, it is good practice to keep an ongoing, up-to-date record of this in their

Section 7: Consent and confidentiality

formal record. This might include a summary of your discussions, the outcomes of those discussions and any decisions made. If you are employed, your employer may use consent forms or have other procedures in place.

– **Implied consent**
  This is where consent from the service user is not expressly spoken or written but can be taken as understood, for example because they have agreed to receive treatment, care or other services. If you are using identifiable information to care for a service user or provide services to them, in most circumstances you will have their implied consent. Most service users will understand the importance of sharing information within the multidisciplinary team. If you are not sure whether you have implied consent, you should always get express consent.

The DPA deals with the issue of consent. You can find more information in annex A.

Capacity

You must keep up to date and follow the law in this area. If you are employed you should also take account of your employer's policies and processes. If you are self-employed or unsure about a specific situation, you should speak to your professional body or get legal advice.

Examples of reasons an adult service user might lack capacity include:

– a mental-health condition;
– dementia;
– severe learning disabilities;
– brain damage, for example from a stroke;
– a physical or mental condition that causes confusion, drowsiness or loss of consciousness; and
– the effects of alcohol or drugs.

You should assume that adult service users have sufficient capacity unless there is significant evidence to suggest otherwise.

Children and young people

For children under 16, you may need to get consent from someone with parental responsibility. This could be:

– the child's mother or father;
– the child's legally appointed guardian;
– a person with a residence order for the child;
– a local authority designated to care for the child; or
– a local authority or person with an emergency protection order for the child.

However, some children under 16 can give consent if they can fully understand the information given to them. This is known as 'Gillick competence'.

You should treat young people (aged 16 and 17) in the same way as adults and presume they have capacity unless there is significant evidence to suggest otherwise.

Section 7:
Consent and confidentiality

Making decisions for people who lack capacity

The law surrounding making decisions on behalf of a person who lacks capacity varies among the UK countries.

In England, Wales and Northern Ireland, the law says you must act in the 'best interests' of service users. This includes giving service users who have capacity enough information to make sure that they are able to make a decision about whether they will allow you to share their information with other people.

Both the Mental Capacity Act 2005 and the Mental Capacity Act (Northern Ireland) 2016 set out what you should consider when making 'best interests' decisions on behalf of someone who lacks capacity. You should:

- consider all the circumstances relevant to the service user, for example the type of mental-health condition or physical illness they have;
- consider whether they are likely to have capacity in the near future and if the decision can be postponed until then;
- involve them as far as possible;
- take account of the beliefs, values, wishes and instructions they expressed when they had capacity; and
- be aware of the views of, for example, their close relatives, carers and guardians.

However, you need to balance the best interests of the service user against other duties. If you have a legal duty to share the information, or need to share it to protect the public interest, you can share it without the consent of the service user. We explain this in more detail later in this document.

In Scotland, the Adults with Incapacity (Scotland) Act 2000 sets out the principles you must follow when making decisions on behalf of someone without capacity.

1. Any action or decision you take must benefit the person and must only be taken when you cannot reasonably achieve that benefit otherwise.

2. Any action or decision you take should be the minimum necessary.

3. You must take account of the present and past wishes and feelings of the person, as far as possible.

4. You should take account of the views of others who have an interest in the person's welfare.

5. You should encourage the person and allow them to make their own decisions and manage their own affairs as much as possible and develop the skills needed to do so.

Section 8:
Disclosing information with consent

In most cases, you will need to make sure you have consent from the service user before you disclose or share any identifiable information.

Working with other practitioners

One of the most common reasons for disclosing confidential information will be when you contact other health and care practitioners. This might include discussing a case with a colleague or referring a service user to another health and care professional.

Sharing information is part of good practice. Care is rarely provided by just one health and care professional, and sharing information within the multidisciplinary team or with other organisations or agencies is often an important way of making sure care can be provided effectively.

Most service users will understand the importance of sharing information with others who are involved in their care or treatment and will expect you to do so, so you will normally have implied consent to do this.

However, when you share information with other colleagues, you should make sure that:
– it is necessary to provide the information;
– you only disclose the information that is relevant; and
– the professional receiving the information understands why you are sharing it and that they have a duty to keep it confidential.

If you decide not to contact other practitioners when you might reasonably be expected to, or if a service user asks you not to, it is important that you keep clear records of this and are able to justify your decision.

If you are concerned about a request someone makes for information – for example, you think the information they have asked for is not relevant – you should contact the person who has asked for the information so they can explain their request. You may also want to get legal advice, or advice from a union or professional body if you are a member.

Other reasons

It is important that you get express consent, in writing where possible, if you plan to use identifiable information for reasons which are not directly related to the service user's care or if they would not reasonably expect their information to be used or shared in that way.

Examples might be where you need information for research, teaching or health and care services planning. In many cases it will be sufficient to use information which does not identify the service user. Where possible, it is better to use this than to use identifiable information. You should consider how much information you need to change or remove to make sure that you are protecting the service user's confidentiality. For example, you should consider whether the area you work in means that it might be possible to identify the service user by their job or by their medical condition.

If you need to use identifiable information, you should explain fully to the service user how you will use their information and whether there are any risks involved in disclosing it. You should make sure that their consent is clearly recorded in their notes.

Sometimes, a third party who is not a health and care professional may ask you for information. This might be a request to send information to an insurance company, government agency or a solicitor. You should make sure that you have express consent to provide any information.

Section 8:
Disclosing information with consent

In these situations, you should also keep a written record of the information you have disclosed and only disclose what you have been asked to. You should also offer to show the service user or provide a copy of any report you write about them for such purposes.

If a service user does not give their consent

You should make sure that you explain to the service user the possible effect of not sharing information about their care or other services you are providing.

If a service user who has capacity refuses to give consent for information to be shared with other health and care professionals involved in providing care, treatment or other services, you must respect their decision, even if it could negatively affect the care, treatment or other services they can receive.

However, if the law says you must disclose the information or it is justified in the public interest to do so, you can do so without the consent of the service user. We explain more about situations like this later in this document.

Section 9:
Disclosing information without consent

There are a small number of circumstances where you might need to pass on information without consent, or when you have asked for consent but the service user has refused it.

If the service user is unable to give their consent

In some circumstances it may not be possible to get consent from a service user to share information. For example, in some emergency situations, they may be unable to communicate or give consent because they are very unwell or unconscious. In other circumstances, they may not have capacity to give consent.

As discussed earlier, whether a service user has capacity will depend on a number of things, including their mental capacity and age. If a service user is unable to give consent, you may have to disclose information if it is in their best interests. We have outlined earlier in this guidance what you will need to consider when deciding whether it is in their best interests.

Also, you may need to share information with those closest to them (such as a carer or family members) so that you or other health and care professionals can decide what is in their best interests. It is also reasonable to assume that they would want those closest to them to be kept informed of their condition, treatment or care, unless they have previously said otherwise.

You should speak to your employer (if you have one) or professional body for further guidance.

Public interest

You can also disclose confidential information without consent from the service user if it is in the 'public interest' to do so.

This might be in circumstances where disclosing the information is necessary to prevent a serious crime or serious harm to other people. You can find out whether it is in the public interest to disclose information by considering the possible risk of harm to other people if you do not pass it on, compared with the possible consequences if you do. This includes taking account of how disclosing the information could affect the care, treatment or other services you provide to the service user.

You should carefully consider whether it is in the public interest to disclose the information. If you are unsure, speak to your manager or employer (if you have one), or your union or defence organisation. You may also want to get legal advice.

You need to be able to justify a decision to disclose information in the public interest (or a decision not to disclose information) so it is important that you keep clear records.

Even where it is considered to be in the public interest to disclose confidential information, you should still take appropriate steps to get the service user's consent (if possible) before you do so. You should keep them informed about the situation as much as you can. However, this might not be possible or appropriate in some circumstances, such as when you disclose information to prevent or report a serious crime.

Section 10:
Disclosing information by law

Sometimes, you may be asked for information directly under the law – for example, if a court has ordered you to disclose the information. You have a legal duty to keep to orders made by the court.

You should tell the service user if you have had to disclose information about them by law, unless there are good reasons not to – for example, if telling them would affect how serious crime is prevented or detected. You should also only provide the information you have been asked for and keep a record of this.

Keep in mind that not all requests from solicitors, the police or a court are made under a legal power that means you must disclose information. If disclosure is not required by law, and cannot be justified in the public interest, you must get express consent from the service user.

Requests from service users

Service users have the right to see information you hold about them and it is important that you respect this.

Safeguarding

Our standards of conduct, performance and ethics say that:

'You must take appropriate action if you have concerns about the safety or well-being of children or vulnerable adults.' (7.3)

In these situations, the following apply.

– If you are employed, you should follow local policies and processes for raising a safeguarding concern. This might include informing the local council or the police.
– If you are self-employed and you are concerned that someone has caused harm, or could pose a risk to vulnerable groups, you should refer the matter to the Disclosure and Barring Service, or in Scotland, Disclosure Scotland. You may also want to inform the local council or the police.

Section 11:
Disclosing information to regulators

There are a number of regulators – such as the General Medical Council, the Care Quality Commission and us – who may need you to pass on information to them. In some cases regulators have statutory powers to request information (see 'Identifiable information and fitness to practise' below). This section refers to regulators of health and care professionals, but is relevant to other types of regulators as well.

Reporting your concerns

Registrants are often not sure about passing on identifiable information because they do not know how this information might be used. However, so that regulators can protect the public, it is important that you tell them if you have any concerns about whether a registered professional is fit to practise. This is also related to your duties under our standards of conduct, performance and ethics.

When you tell a regulator about your concerns, you may need to include information about a service user. This might be because your concerns are about the care or services provided to a particular service user or group of service users.

If you need to disclose information about a service user, make sure that the information is relevant to your concerns. You should, if possible, remove all identifiable information, including names and addresses. Where it is necessary to include identifiable information it is good practice to tell the service user and try to get their consent for the disclosure. However, if the disclosure is required in the public interest, identifiable data can be disclosed without consent.

You should keep an appropriate record of any disclosures, giving reasons for disclosing the information and a justification for that disclosure where possible.

You might also want to discuss these matters with your manager (if you have one) or a professional colleague.

If you are not sure whether to tell a regulator, what information to provide, or how they will use the information, you should contact the regulator for more advice.

Identifiable information and fitness to practise

Sometimes regulators make requests for information about service users that they need to help them investigate a registrant's fitness to practise. For example, if we are looking at a complaint about a registrant's record-keeping, we might need to ask for copies of the records so that we can decide whether the professional has met our standards.

Regulators often have powers to require information from people other than the person being investigated. They will sometimes make these requests using 'statutory powers'. These are powers that a regulator has by law to help them in an investigation. You have to provide the information, but it is good practice to tell service users (if possible) when you have disclosed information about them.

You should make sure that you only provide the information the regulator has asked for, and provide anonymised or partly anonymised information when you can.

If we ask for information using our statutory powers, we will put this in writing and explain why

Section 11: Disclosing information to regulators

we are asking for it and how we will use it. Information we use during a hearing will usually have all the identifiable information removed from it, and we will always take appropriate steps to make sure that we protect a service user's confidentiality. The law says we have to handle this information responsibly. For example, we use terms such as 'Service user A' to refer to individuals. We may also hold hearings fully or partly in private when necessary.

Section 12:
Confidentiality and accountability

As a health and care professional, you are responsible and accountable for the decisions you make, including ones about confidentiality and disclosing information.

We feel that you are best placed to make practical decisions, taking account of the way in which you practise. You need to make informed and reasonable decisions about your own practice to make sure that you always respect and protect the confidentiality of service users. It is also important that you are able to justify the decisions you make.

If you are employed by an organisation, they are likely to have policies and procedures in place relating to confidentiality. We expect you to practise in line with these.

If you are self-employed or employ other people, we expect you to put in place policies and procedures to make sure you are holding service users' information confidentially and sharing it only where lawful and appropriate.

However, if you find that the policies and procedures relating to confidentiality in the organisation or service where you work are not suitable or appropriate, or do not allow you to carry out your duties, you should raise your concerns. This might be to your manager or the person with responsibility for data protection where you work, or with another appropriate authority. If you feel that your employer's policy might mean that confidentiality is put at risk, you should contact your union, professional body or us for advice.

Section 13:
More information

If you are not sure about what you should do in a specific situation, consider asking your employer, professional body or independent legal representative for advice.

The **Information Commissioner's Office (ICO)** is the UK's independent authority set up to uphold information rights and has produced guidance which you may find useful: https://ico.org.uk/

We also recognise the valuable role professional bodies play in providing advice and guidance to their members. If you are a member of a professional body, you may find it useful to ask for advice about good practice on confidentiality as it relates to your profession.

In particularly complex situations, you might also consider getting independent legal advice.

Contact us

You can contact us if you have any questions about this guidance or what we expect with regard to confidentiality. However, we cannot offer legal advice. Our contact details are below.

The Health and Care Professions Council
Park House
184 Kennington Park Road
London
SE11 4BU

Phone: +44 (0)300 500 6184

You can download copies of our standards documents and other publications from our website at www.hcpc-uk.org

Glossary

You may not be familiar with some of the terms we use throughout this document, so we have explained them below.

Accountable
As an accountable health and care professional, you will be responsible for the decisions you make and you may also be asked to justify them.

Anonymised information
Information about a service user that has had all identifiable information removed from it, and where there is little or no risk of an individual being identified.

Autonomous
As an autonomous health and care professional, you make your own decisions based on your own judgement.

Court order
An order made by a judge or court for something to happen.

Disclose, disclosure
When information is revealed, released or passed on from one person to another.

Express consent
Specific permission from the service user, given verbally or in writing, to use or share information about them.

Fitness to practise
A professional is fit to practise if they have the training, skills, knowledge, character and health to do their job safely and effectively. We can take action if we have concerns about a registrant's fitness to practise.

Identifiable information
Any information that might identify a service user, for example their name, address or details of their health condition, treatment or care.

Implied consent
When a service user is aware of the possibilities for sharing information and their right to refuse this, but does not object.

Informed consent
When a service user has enough information to make a decision about whether they give their permission for information to be shared with other people.

Professional bodies
Organisations which promote or represent members of a profession. They may also provide guidance and advice, produce curriculum frameworks, oversee post-registration education and training, and run continuing professional development (CPD) programmes.

Public interest
Disclosures of information are made in the 'public interest' when it is necessary to prevent a serious threat to public health, national security, the life of the person concerned or another person, or to prevent or detect serious crime.

Register
A published list of health and care professionals who meet our standards. The Register is available on our website at www.hcpc-uk.org

Registrant
A health and care professional who appears on our Register and meets our standards.

Regulator
An organisation that protects the public by making sure people or organisations keep to certain laws or requirements.

Glossary

Service user
Anyone who uses or is affected by the services of a registrant. This includes patients and clients.

Standards of conduct, performance and ethics
Standards of behaviour that we expect from health and care professionals who are registered with us.

Statutory powers
Certain organisations, such as regulators, have powers under legislation. This sometimes includes the power to ask for information from people.

Third party
Someone who is not the service user, a member of their family or a carer or the professional involved in their care or treatment. This could include another professional or an organisation that has requested information.

Annex A:
Data protection principles

(Plain English Campaign's Crystal Mark does not apply to annex A or its glossary.)

The General Data Protection Regulation (GDPR), supported by the Data Protection Act 2018 (DPA) governs how personal data (any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier), including service user records, should be handled.

GDPR principles

GDPR sets out seven key principles, which are broadly similar to the Data Protection Act 1998 (the 1998 Act):

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality (security).
- Accountability. (This is the most substantial change when compared with the 1998 Act).

Lawful basis for processing

You must have at least one lawful bases for processing personal data:

- **Consent:** the individual has given unambiguous consent and for a specified purpose.
- **Contract:** it is necessary under a contract, or as a prerequisite.
- **Legal obligation**.
- **Vital interests:** it is necessary to protect someone's life.
- **Public task:** it is required in the public interest or for an official function.
- **Legitimate interests:** it is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data.

Consent

Consent is one of the six lawful bases for processing personal data and must:

- be unambiguous;
- involve a clear affirmative action
- be prominent, concise and easy to understand and separate from terms and conditions;
- where explicit, be expressed in words; and
- cover the controller's name, the purposes of processing and the types of processing activity.

Purpose limitation

This principle seeks to make sure you are open and transparent about why you are collecting personal data, and that you use that data in a way the individual reasonably expected you to.

In order to satisfy this principle, you must:

- know why you are collecting personal data, and what you will do with it;
- clearly explain why you are collecting personal data, and what you will do with it; and
- only use or disclose information outside of this purpose if it is lawful or transparent.

Data minimisation

You must make sure any personal data you are processing is:

- adequate (to enable you to discharge the intended purpose);
- relevant (has an appropriate link to that purpose); and
- limited (you don't hold any more information than you absolutely need for that purpose).

Annex A:
Data protection principles

Accuracy
You should take reasonable steps to make sure any personal data you hold is accurate and:

– keep it updated as appropriate;
– correct or erase it as appropriate; and
– carefully consider any challenges to the accuracy of the data.

Storage limitation
You must not keep personal data for any longer than you need it. You should:

– be able to justify how long you keep personal data;
– have a clear policy on retention periods;
– regularly review your data to assess whether it needs to be deleted or anonymised;
– consider requests for personal data to be erased on a case by case basis.

Integrity and confidentiality (security)
You must process personal data securely, and ensure you have:

– undertaken an appropriate risk analysis;
– developed a clear policy; and
– considered both physical and technical data.

Accountability
You are responsible for the way you process and store personal data. You have duty to comply with the principles of the GDPR, and should be able to evidence how you do so.

Where to go for further advice and support
The Information Commissioners Office (ICO) is the leading authority in the UK for data protection. It has a number of helpful resources on its website:

– A Guide the General Data Protection Regulation.
– Health and social care FAQs.
– FAQs or small health sector bodies.

Park House
184 Kennington Park Road
London SE11 4BU

tel +44 (0)300 500 6184
fax +44 (0)20 7820 9684
www.hcpc-uk.org

To request this document in Welsh or an alternative format, email publications@hcpc-uk.org

Publication code: 20080206dPOLPUB (revised October 2018)